

TESTUDO

HORIZON-CL3-2022-INFRA-01- Grant Agreement No. 101121258

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES IN
INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

D11.3

Exploitation plans and impact pathways assessment

Lead Beneficiary	DBC
Type of Deliverable	R
Version	1.6
Due date	31.03.2025
Date of submission	31.03.2025
Dissemination level	PU



Work Package	WP1 – Impact creation and outreach v1
Deliverable	D11.3 – Exploitation plans and impact pathways assessment
Editor (s)	Erika Nika - DBC
Contributor (s)	Polyxeni Chrysostomide – ACCELI Christiana Themistocleous - ACCELI
Reviewer (s)	Anastasios Dimou – CERTH Kostas Peroulis - EYDAP

Abstract	<p>This document will report the developed exploitation plan along with the definition of actions to increase impact and their assessment.</p> <p>This deliverable further provides the first version of the market analysis for the existing systems and commercial products and aims to set up effective business models for TESTUDO.</p>
Keywords	Exploitation Plan, Exploitable Results, Market Analysis, Business Models
Disclaimer	<p>The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.</p> <p>© Copyright in this document remains under the TESTUDO consortium</p>

Document History

Version	Date	Partner	Remarks
0.1	16.12.2024	DBC	ToC
0.2	03.02.2025	ACCELI	First draft regarding market analysis.
1.0	12.02.2025	DBC	Final draft sent for internal review
1.3	14.03.2025	DBC, ACCELI	Pre-Final version after feedback received
1.4	24.03.2025	CERTH	Quality control
1.5	26.03.2025	DBC, ACCELI	Final version
1.6	31.03.2025	CERTH	Submission

Executive Summary

The TESTUDO project, funded under Horizon Europe, aims to enhance Critical Infrastructure (CI) protection through an autonomous swarm of heterogeneous resources for threat prediction and prevention. By integrating AI-driven surveillance, unmanned aerial and ground vehicles (UAVs & UGVs), cybersecurity measures, and digital twins, the project develops an advanced security framework for real-time threat detection, response, and situational awareness.

This document presents the exploitation strategy and impact pathways assessment for TESTUDO, ensuring that the developed technologies achieve long-term sustainability, commercialization, and industrial application. It provides a structured approach to:

- Identifying exploitable results (ERs)
- Defining intellectual property rights (IPR) management
- Assessing market conditions
- Mapping strategic stakeholders for the future deployment of TESTUDO technologies

Additionally, this document lays the groundwork for the next deliverable, as specified in the document.

The analysis begins with a comprehensive review of the project's exploitable results, highlighting the contributions of each partner. These results range from AI-powered surveillance modules, cybersecurity solutions, multispectral detection systems, UAV and UGV platforms, and digital twins. The document outlines their technology readiness levels (TRLs) and potential market applications, ensuring each innovation is positioned for commercial uptake, integration into existing security frameworks, or further research and development.

The IPR management strategy ensures that intellectual assets generated within the project are appropriately protected and utilized. The consortium follows a structured framework for ownership, access rights, and commercialization, balancing open knowledge dissemination with proprietary protection. Various legal instruments such as patents, copyrights, and licensing agreements safeguard project outcomes while fostering collaboration between research institutions and industry partners.

A preliminary market and competition analysis assesses the business environment and industry dynamics affecting TESTUDO's deployment. The report identifies key technological trends, including advancements in AI, IoT, cybersecurity, and digital twins, shaping the landscape for autonomous security solutions. The competitive analysis benchmarks TESTUDO against existing market players, research initiatives, and alternative solutions, ensuring the project maintains a competitive advantage in CI protection.

The document also includes a socioeconomic impact assessment using PESTLE and SWOT analysis methodologies. The PESTLE analysis evaluates the political, economic, social, technological, legal, and environmental factors that influence the adoption of TESTUDO technologies. It highlights regulatory challenges, public perception concerns, cybersecurity threats, and funding opportunities within the European Union's security framework. The SWOT analysis further identifies the strengths, weaknesses, opportunities, and threats associated with TESTUDO, providing a strategic roadmap for maximizing its impact.

Stakeholder identification and analysis are crucial to the project's exploitation strategy. Public sector regulatory bodies, industry leaders, research institutions, law enforcement agencies, and civil society groups are key stakeholders. The report outlines engagement strategies to ensure compliance with EU security policies, facilitate industry adoption, and address ethical concerns about AI surveillance and data privacy.

Individual exploitation plans are developed for each project partner, detailing their intended commercialization or research pathways. Some partners focus on direct market entry through licensing agreements and technology spin-offs, while others prioritize further R&D collaborations or integration into existing security solutions. The expected time to market varies across technologies, with most exploitable results reaching commercialization within two to four years.

The TESTUDO project's long-term success depends on effectively translating research innovations into real-world applications. The exploitation strategy provides a structured framework for ensuring that TESTUDO technologies are adopted by industry, integrated into regulatory frameworks, and aligned with emerging security challenges. The ongoing refinement of business models and stakeholder engagement strategies will strengthen TESTUDO's position as a leading autonomous security and CI protection initiative.

Table of Contents

1. Introduction	9
1.1. Purpose and Scope.....	9
1.2. Approach for Work Package and Relation to Other Work Packages and Deliverables	9
1.3. Methodology and Structure of the Deliverable	10
2. Exploitable Results Description gathered from Project Partners	12
3. IPR Management.....	31
3.1. Types of Knowledge	31
3.2. Record of Intellectual Property Assets.....	34
3.3. Ownership Schemas.....	35
3.4. IPR Matrix.....	38
3.5. Instruments for Project Results Protection	41
3.6. Management of Knowledge.....	43
3.7. Project Results Protection.....	45
4. Preliminary Market and Competition Analysis	49
4.1. Business Environment.....	49
4.2. Benefits to the Industry, Market Players, and to the Economy.....	49
4.3. Policy Plans & Regulatory Framework	50
4.3.1. Unmanned Aircraft Vehicles (UAVs).....	50
4.3.2. GDPR.....	51
4.3.3. AI act by European Commission	51
4.3.4. Other relevant legislations and standards	51
4.4. Technology Trends	53
4.5. Competitive Landscape.....	53
4.5.1. Market Analysis Survey	54
5. Socioeconomic Analysis	59
5.1. Project PESTLE Analysis.....	59
5.2. Project SWOT Analysis	61
6. Stakeholder Identification and Analysis.....	65
6.1. Types of Stakeholders Characterization	65
6.2. Stakeholders Analysis.....	66
7. Individual Exploitation Plans	69

8. Conclusions	72
References	74
Annex 1 – Template for Market Analysis Report - Partners Fill-In Form	75
Annex 2 – Key innovative technologies	82
Annex 3 – Benefits to the Industry, Market Players and to the Economy – Contributions from partners	87
Annex 3 – Lists of current technology trends which are relevant to the innovations being developed in TESTUDO	96
Annex 4 – Competitive landscape.....	107
Annex 5 – Market Analysis Survey	126

List of Figures

Figure 1. Target Customer.	55
Figure 2. Broader customers.....	55
Figure 3. Description of the market.....	56
Figure 4. Market size.....	57
Figure 5. Competitors.	57
Figure 6. Alternatives/Competition to exploitable assets.	58
Figure 7. Maturity of current competition.	58
Figure 8. Europe Drone Market Revenue Share (2021).....	96
Figure 9. North America 3D Mapping & 3D Modelling Market Size, 2019-2032 (USD Billion).	97
Figure 10. Thermal Imaging Market size, 2022 to 2032 (USD Billion).	98
Figure 11 Attractive Opportunities in Thermal Imaging Market.	99
Figure 12 U.S Recognition Market.	100
Figure 13. Digital Twin Market Share, By End-Use 2022 (%).	101
Figure 14. Industries using DTs.	102
Figure 15. Impact of Digital Twins solutions in the business world.....	102
Figure 16. KI Engineering Solution.....	111

List of Tables

Table 1. Exploitable Results Overview	30
Table 2. IPR Matrix.....	41
Table 3. SWOT Analysis Template.	62
Table 4. SWOT Analysis.....	64

Terms and Abbreviations

Label	Text
AI	Artificial Intelligence
AoE	Autonomy on the Edge
AoP	Autonomy on the Platform
AR	Augmented reality
BIM	Building Information Modelling
BVLOS	Beyond the visual line of sight
CAGR	Compound Annual Growth Rate
CI	Critical Infrastructure
CSIM	Converged Security Information Management
DT	Digital Twins
DVR	Design Verification Report
EASA	European Union Aviation Safety Agency
EvONET	Evolutionary state graph network
FAA	Federal Aviation Administration
GDPR	General Data Protection Regulation
GIS	Geographic Information System
HAPS	High Altitude Platform Station
HMI	Human-Machine Interface
IDS	Intrusion Detection System
IoT	Internet of Things
I-TO-I	Testing Imaging Transition of Information
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LIDAR	Light Detection and Ranging
LUC	Light UAS operator Certificate
ML	Machine Learning
NDR	Network Detection and Response
NIR	Near Infrared Spectrum
OSOs	Operational Safety Objectives
RoHS	Restriction of Hazardous Substances
RTC	Restricted Type Certificate
SAIL	Specific Assurance and Integrity Level
SOC	Security Operations Centres
TAF-BW	Test Area Autonomous Driving Baden Württemberg
TC	Type Certificate
TOM	Time of Flight
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
VRUs	Vulnerable Road Users
WEEE	Waste Electrical and Electronic Equipment

1. Introduction

1.1. Purpose and Scope

This deliverable provides a comprehensive exploitation strategy and impact pathways assessment for the TESTUDO project. TESTUDO, funded under Horizon Europe, is an initiative to enhance critical infrastructure protection through an autonomous swarm of heterogeneous resources for threat prediction and prevention. The project integrates AI-driven surveillance, unmanned aerial and ground vehicles (UAVs & UGVs), cybersecurity measures, and digital twins to develop a next-generation security framework for real-time threat detection, response, and situational awareness.

This document outlines the approaches for maximizing the impact of the project's results by defining key Exploitable Results (ERs), Intellectual Property Rights (IPR) management, business models, and market readiness strategies. It provides stakeholders with a roadmap for ensuring that TESTUDO's outcomes translate into viable technological innovations that support real-world applications in security, defence, emergency response, and infrastructure resilience.

This deliverable's scope covers identifying exploitable results, market analysis, stakeholder engagement strategies, and commercialization pathways. It also examines the project's alignment with regulatory frameworks, particularly in AI ethics, cybersecurity laws, and UAV regulations. This document is a foundational step for the final market analysis, impact assessment, and policy recommendations presented in future deliverables (D12.2).

1.2. Approach for Work Package and Relation to Other Work Packages and Deliverables

This deliverable is part of Work Package 11 (WP11) – Impact Creation and Outreach, which focuses on defining TESTUDO's long-term exploitation potential, ensuring sustainability, and enhancing its outreach to relevant market stakeholders. WP11 ensures that the innovative solutions developed within TESTUDO achieve maximum impact by establishing a clear strategy for their adoption, commercialization, and integration into existing security ecosystems.

D11.3 is closely linked to other deliverables and work packages within TESTUDO, particularly those related to technological development, market deployment, and policy frameworks. The key interdependencies are:

- WP4 – AI-Driven Surveillance and Threat Prevention (M3–M18) transitions into WP5 – Augmented Sensing and Communications for Effective Autonomy v2 (M19–M33). WP5 further enhances AI-powered threat detection, digital twins, UAV and UGV coordination, and cybersecurity frameworks. D11.3 evaluates the exploitation potential of these technologies and identifies market adoption pathways.
- WP6 – AI-powered Threat Identification (M3–M18) transitions into WP7 – Artificial Cognitive Intelligence for Threat Identification v2 (M19–M33). WP7 continues developing advanced AI techniques for security threats, including refining innovative detection methods and optimizing

data processing. D11.3 evaluates these solutions' commercial viability and compliance with intellectual property regulations.

- WP8 – Predictive Intelligence, Operational Support, and Platform Implementation (M4–M18) transitions into WP9 – Predictive Intelligence, Operational Support, and Platform Implementation v2 (M19–M34). WP9 ensures continued alignment with European cybersecurity laws, AI ethics frameworks, and UAV regulations, which are crucial for market entry. D11.3 integrates insights from WP9 to propose policy recommendations and compliance strategies.
- WP10 – Large-scale Pilot Execution and Evaluation (M6–M18) transitions into WP11 – Large-scale Validation and Refinement of Use Cases (M19–M36). WP10 is crucial in further validating TESTUDO technologies through extended real-world demonstrations. The results from pilot use cases provide critical insights into end-user adoption, system performance, and regulatory alignment, directly informing D11.3's exploitation pathways.
- WP12—Market Analysis and Policy Recommendations (M19–M36) builds upon the initial steps defined in WP11 – Impact Creation and Outreach v1 (M1–M18). D11.3 lays the groundwork for TESTUDO's business models, competition landscape, and commercialization pathways, while D12.2 (produced in WP12) will deliver the final impact assessment and policy recommendations.

1.3. Methodology and Structure of the Deliverable

The methodology for this deliverable follows a structured approach to exploitation planning and impact assessment, ensuring that TESTUDO's technological outcomes are effectively mapped to market needs and regulatory environments. Given that WP10 and Task 10.4 focus on user evaluation and acceptance, the findings from these activities will be directly integrated into the exploitation strategy. User feedback collected through pilot demonstrations, usability assessments, and real-world testing will be crucial in shaping commercialization pathways. By incorporating user knowledge, the impact assessment will consider market conditions and regulations and ensure that TESTUDO technologies are aligned with real-world operational requirements and stakeholder expectations.

1. **Exploitable Results Identification and Classification.** The first step involves gathering ERs from project partners. These ERs are assessed based on their technology readiness levels (TRLs), competitive positioning, and commercialization potential.
2. **Intellectual Property Rights (IPR) Strategy.** An IPR framework is established to define ownership, licensing models, and protection mechanisms for project innovations. This ensures that TESTUDO's research outputs are secured while enabling commercial partnerships and collaborations.
3. **Market Analysis and Business Model Development.** A market analysis evaluates the demand for TESTUDO's solutions, identifies competitors, and assesses industry trends. Business models are developed to outline potential revenue streams, adoption strategies, and partnerships.
4. **Stakeholder Engagement and Policy Alignment.** A detailed stakeholder analysis maps key market players, regulatory bodies, and industry partners. The project's compliance with EU security

regulations, AI ethics policies, and UAV operational frameworks is assessed to facilitate smooth market entry.

5. Impact Pathways and Exploitation Roadmap. The final phase outlines a roadmap for exploitation, detailing the steps required for commercialization, technology transfer, and further research collaboration. This includes timelines for market deployment, pilot implementation feedback loops, and strategic partnerships.

The deliverable is structured as follows:

- Section 2: Exploitable Results (ERs) Description – A detailed breakdown of TESTUDO’s ERs, TRLs, and commercialization potential.
- Section 3: IPR Management – A structured ownership, licensing, and knowledge protection framework.
- Section 4: Market and Competition Analysis – Evaluation of business opportunities, industry demand, and competitive positioning.
- Section 5: Socioeconomic and Regulatory Impact – PESTLE and SWOT analysis to assess external factors influencing market adoption.
- Section 6: Stakeholder Identification and Engagement – Mapping key stakeholders and strategies for effective collaboration.
- Section 7: Individual Exploitation Plans – Partner-specific plans for utilizing TESTUDO’s ERs.
- Section 8: Conclusions—This is the Final assessment of the exploitation potential and the next steps for TESTUDO’s commercialization and policy integration.

2. Exploitable Results Description gathered from Project Partners

As part of the TESTUDO project, we collected and analysed Exploitable Results (ERs) submitted by the project partners to highlight the innovative outputs and their potential impact. This structured effort aimed to ensure that all results produced during the project were effectively aligned with its goals, assessed for readiness, and prepared for practical application or commercialization.

The collection process involved a specially designed exploitation tool (Exploitation Tool) based on Excel, which provided a unified framework for partners to submit detailed information about their contributions. Each partner was asked to complete a comprehensive set of fields, including the ER's name, category, short description, Technology Readiness Level (TRL) progression, strengths, weaknesses, market opportunities, risks, and the envisioned path to market.

A key focus was understanding how these results could be leveraged within organizations, such as extending product portfolios, developing new solutions, or addressing specific market needs. Additionally, the data provided insights into the ERs' competitive positioning, highlighting areas of innovation and identifying potential challenges, such as market competition or resource dependencies.

This initial evaluation is a preliminary approach to collecting and organizing Key Exploitable Results (KERs). A detailed assessment of all ERs will be conducted in a subsequent phase (Spring 2025) to finalize the selection of KERs. This phased process ensures a thorough and strategic review, allowing for the identification of results with the highest potential for impact and scalability.

Below, we present the ERs collected from the project partners for a detailed review:

ER1: Maximized Surveillance Swarm Intelligence Module

The Maximized Surveillance Swarm Intelligence Module is a software component designed to implement an algorithm for surveillance of a defined area using a heterogeneous fleet of UAVs and UGVs¹. It was suggested by SINTEF, the sole owner, with no other contributors. The module is developed within tasks T4.4, T5.4, T4.5, and T5.5 as specified in the Grant Agreement. At the start of the project, its Technology Readiness Level (TRL) was 4, and it is expected to reach TRL 7 by completion. This result falls under the category of technical research with the potential for more efficient use of available resources. The module excels in planning actions and missions to maximize surveillance efficiency, but its integration with heterogeneous hardware remains challenging. It faces competition from Anduril's Lattice system (Anduril Industries, n.d.) (an AI-powered autonomous security platform used for persistent surveillance, threat detection, and autonomous drone coordination in defence and critical infrastructure applications) and targets markets such as critical infrastructure, the defence sector, search and rescue, agriculture, and forestry. The estimated time to market is four years. SINTEF, as a non-profit organization, aims to embed the results into its knowledge base for future research activities, with spin-out opportunities considered as the technology matures. This is regarded as a Key Exploitable Result (KER).

¹ By 'heterogeneous,' we refer to a diverse mix of aerial and ground-based robotic platforms that differ in size, mobility, sensor capabilities, autonomy levels, and communication protocols. This module ensures seamless coordination between fixed-wing and rotary UAVs for wide-area reconnaissance and UGVs for detailed ground-level assessments, maximizing surveillance effectiveness across complex operational environments.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: SINTEF (sole owner).
- Market: Critical infrastructure, defence, search & rescue, agriculture, forestry.
- Time to Market: 4 years.
- Potential as KER.

ER2: Autonomous Resource Allocator Module

The Autonomous Resource Allocator Module is a software component that implements an algorithm for allocating resources, such as UAVs, UGVs, sensor nodes, communication networks, and energy supplies for surveillance of an area. SINTEF, the sole owner, suggested and developed the module without additional contributors. It is linked to tasks T4.4, T5.4, T4.5, and T5.5 in the Grant Agreement. The module started at TRL 4 and is expected to reach TRL 7 by the project's end. It is categorized under technical research and aims to optimize the use of resources by assigning them efficiently based on performance and capabilities. The module's strengths include dynamically matching resource allocation to demand, though challenges remain in ensuring smooth integration with heterogeneous hardware. The leading competitor is Anduril's Lattice system. The targeted market consists of critical infrastructure, the defence sector, search and rescue, agriculture, and forestry, with an estimated time to market of four years. SINTEF, as a non-profit, intends to extend its knowledge base with this result, incorporating it into new research activities and considering potential spin-outs as the technology evolves. This is classified as a KER.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: SINTEF (sole owner).
- Market: Critical infrastructure, defence, search & rescue, agriculture, forestry.
- Time to Market: 4 years.
- Potential as KER.

ER3: Network Infrastructure

The Network Infrastructure module is a software component that manages the wireless multi-hop communications infrastructure. It was suggested and developed by CEA, the sole owner, with no additional contributors. The module is associated with task T4.5 in the Grant Agreement. At the start of the project, it had a TRL of 4 and is projected to reach TRL 7 by its conclusion. This result is categorized under technical research, development, and use in future projects. It allows interaction with more complex systems and supports dynamic network configuration management. Its main strengths include

seamless integration with robotic platforms, though challenges exist in integrating it with onboard drone hardware. The targeted customers include drone operators, critical infrastructure owners, and defence and security organizations. The estimated time to market is four years. CEA, a non-profit organization, intends to extend its R&D portfolio to support the robotics industry and build know-how. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: CEA (sole owner).
- Market: Drone operators, critical infrastructure, defence, security organizations.
- Strengths: Seamless integration with robotic platforms.
- Challenges: Integration with on board drone hardware.
- Time to Market: 4 years.
- Potential as KER.

ER4: Visual Detection Module

The Visual Detection Module is software for detecting relevant objects from video streams. It was suggested and developed by CERTH, the sole owner, with no other contributors. The module is linked to tasks T6.1 and T7.1 in the Grant Agreement. The TRL at the start of the project was 5, with a target of TRL 7 upon completion. The module is categorized under internal use, further research, and future projects to integrate it into more complex solutions. Its strengths include low complexity and high performance, though its robustness in diverse environments has not been thoroughly tested. The market is highly competitive, as computer vision technology is becoming more accessible to non-experts. The primary target customers are law enforcement agencies, first responders for safety applications, and critical infrastructure operators. The estimated time to market is two years. CERTH, as a non-profit organization, plans to extend its expertise and possibly create spin-off companies. This is considered a KER.

Key Information

- TRL: Started at 5, expected to reach 7.
- Owner: CERTH (sole owner).
- Market: Law enforcement, first responders, critical infrastructure operators.
- Strengths: Low complexity, high performance.
- Challenges: Robustness in diverse environments untested.
- Competition: Highly competitive computer vision market.
- Time to Market: 2 years.

- Potential as KER.

ER5: Multispectral Detection Module

The Multispectral Detection Module is a software system for detecting objects from thermal spectrum video streams. It was suggested and developed by CERTH, the sole owner, with no additional contributors. The module is associated with tasks T6.2 and T7.2 in the Grant Agreement. It started with a TRL of 4 and is expected to reach TRL 7 by the project's end. This result is categorized under dataset creation, research promotion, and use in future projects, with the module being a part of more complex systems. Its strengths include high efficiency, but its performance in untested environments remains uncertain. The module's market opportunity is in night vision solutions, with potential competition from existing products. The primary customers include law enforcement agencies, first responders for safety applications, critical infrastructure operators, and security application providers. The estimated time to market is three years. CERTH, a non-profit organization, intends to expand its expertise and consider creating spin-off companies. This is potentially a KER.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: CERTH (sole owner).
- Market: Law enforcement, first responders, critical infrastructure, security applications.
- Strengths: High efficiency in thermal spectrum detection.
- Challenges: Performance in untested environments.
- Competition: Existing night vision solutions.
- Time to Market: 3 years.
- Potential as KER.

ER6: Detection Module on Embedded Platforms

The Detection Module on Embedded Platforms is a software component that enables automatic object detection and identification from video content. It is deployed on UGVs and UAVs, utilizing AI-driven visual image processing capabilities while maintaining low power consumption. TEKNIKER, the sole owner, suggested and developed this module without additional contributors. The relevant tasks from the Grant Agreement are T6.3 and T7.3. The module started at TRL 5 and is expected to reach TRL 7 by the project's completion. It is intended for internal use, further research, and future projects. A key advantage of this module is its ability to provide detection capabilities in low-power, embedded systems. However, it relies heavily on hardware compatibility and may be limited to older neural network architectures. The module targets first responders, autonomous perimeter surveillance (secure boundaries of critical infrastructure, military bases, restricted-access zones, and high-risk areas), area monitoring, and UGV/UAV systems integration. Challenges include the lack of high-quality datasets for embedded models and smooth

integration with heterogeneous hardware. The targeted market includes critical infrastructure, the defence sector, search and rescue, agriculture, and forestry, with an estimated time to market of four years. TEKNIKER, as a non-profit organization, aims to extend its expertise in this field and potentially create spin-off companies. This is considered a possible KER.

Key Information

- TRL: Started at 5, expected to reach 7.
- Owner: TEKNIKER (sole owner).
- Market: Critical infrastructure, defence, search & rescue, agriculture, forestry.
- Strengths: AI-driven detection with low power consumption.
- Challenges: Hardware compatibility, reliance on older neural network architectures.
- Time to Market: 4 years.
- Potential as KER.

ER7: CBRN Detection Tools

The CBRN Detection Tools include an airborne chemical detector with a built-in calibration module to enhance real-time reliability. The module enables qualitative calibration using a reference compound, which continuously adjusts the gas chromatography column times to minimize false positives and negatives. T4i, the sole owner, suggested and developed this result without additional contributors. It is linked to task T6.5 in the Grant Agreement. The TRL at the start of the project was 4, with an expected TRL of 7 at completion. This module is categorized under product development, with high exploitation potential due to the growing demand for real-time chemical detection in CBRN (Chemical, Biological, Radiological, and Nuclear) applications. Its key strengths include adaptability to different UAV types, lightweight design, low power consumption, and real-time detection capabilities. However, challenges include maintenance requirements like battery and molecular sieve changes. The foremost opportunity lies in the increased demand for CBRN monitoring in various sectors, though barriers include a perception that CBRN technologies are complex and require extensive training. Limited competitors are utilizing the GC/PID technique for CBRN events. The targeted market includes tunnel operators, construction companies, fire brigades, police, UAV providers, chemical industries, and environmental agencies. The estimated time to market is three months after project completion. T4i plans to redesign its existing DOVER system to integrate the new built-in unit. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: T4i (sole owner).
- Market: Tunnel operators, construction companies, fire brigades, police, UAV providers, chemical industries, and environmental agencies.

- Strengths: Real-time chemical detection, UAV adaptability, lightweight, low power consumption.
- Challenges: Maintenance needs (battery, molecular sieve changes), perception of complexity.
- Time to Market: 3 months after project completion.
- Potential as KER.

ER8: Cyber-Threat Detection Module

The Cyber-Threat Detection Module is an anomaly-based network intrusion detection system that learns standard network traffic patterns to detect anomalies indicative of cyber-attacks. CEA, the sole owner, suggested and developed this module with no additional contributors. The relevant task from the Grant Agreement is T6.6. The module started at TRL 5 and is expected to reach TRL 7 by the project's completion. It is categorized under internal use, further research, and future projects. A key advantage of the module is its ability to detect unknown threats that may evade signature-based network intrusion detection systems (NIDS). However, high network traffic variability can lead to false positives (i.e., cases where regular network activity is mistakenly identified as a potential cyber threat, triggering unnecessary security alerts and investigations). The module is well-positioned to capitalize on the growing number of zero-day attacks, although the false positive rate presents a challenge. The leading competitor is DarkTrace IDS (Darktrace's Network Detection and Response (NDR) solution utilizes self-learning AI to monitor network traffic for anomalies and potential threats) (Darktrace, 2025). The primary market includes critical infrastructure operators, network operators, and organizations in the defence and security sectors. The estimated time to market is four years. CEA aims to integrate this module into its broader cybersecurity research initiatives as a non-profit organization. This is considered a KER.

Key Information

- TRL: Started at 5, expected to reach 7.
- Owner: CEA (sole owner).
- Market: Critical infrastructure operators, network operators, and defence and security sectors.
- Strengths: Detects unknown threats missed by signature-based NIDS.
- Challenges: High false positive rate due to network traffic variability.
- Time to Market: 4 years.
- Potential as KER.

ER9: Low-Power Hardware Architectures for Machine Vision Applications at the Edge

This module enables AI-powered object detection and identification on the edge for UGVs and UAVs, focusing on low-power consumption. The related tasks from the Grant Agreement are T6.3 and T7.3, both under the ownership of NTTD-IT. The module had a starting TRL of 4 and is projected to reach TRL 7 by the end of the project. It is intended for internal use, further research, and future projects. The main

advantage of this module is its ability to reduce power consumption while maintaining machine vision capabilities. However, challenges include limited testing in real-world edge environments and difficulties integrating with heterogeneous robotic platforms. The targeted market includes first responders, autonomous perimeter surveillance, critical infrastructure, the defence sector, search and rescue, agriculture, and forestry. Starting from the intelligent features that can be extracted from the edge modules deployed on board, another relevant field of application is the cooperation between multiple robotic platform in fleets and peer mode. The estimated time to market is four years. TEKNIKER, as a non-profit organization, aims to advance its expertise in low-power AI-driven hardware and potentially establish spin-off companies. This is considered a possible KER. NTTDATA Italia S.p.A. as part of a large corporation aims to develop, test and evaluate the readiness of such technologies to bring them to market as innovative projects for its clients.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: NTTD-IT.
- Market: First responders, autonomous perimeter surveillance, critical infrastructure, defence, search & rescue, agriculture, and forestry.
- Strengths: AI-powered object detection with low-power consumption.
- Challenges: Limited real-world testing and integration with heterogeneous robotic platforms.
- Time to Market: 4 years.
- Potential as KER.

ER10: Visual Activity Recognition Module

The Visual Activity Recognition Module is a software component that detects abnormal behaviour using static CCTV cameras. The module employs semi-supervised learning methods to train an AI model capable of clustering and identifying both everyday and abnormal situations. It is primarily intended for use cases such as monitoring tunnel traffic and recognizing basic human activities. This module was suggested and developed by VICOM, which is also the sole owner and has no additional contributors. The relevant task of the Grant Agreement is T6.4. It started at TRL 4 and is expected to reach TRL 6 by the project's end. The primary mode of exploitation is through licensing. The module's key strength is its ability to analyse traffic events in real time, but a limitation is its reliance on supervised semantic interpretation for detected events. The module presents opportunities for deployment in video surveillance systems, particularly for CCTV integrators. However, its relatively low practical accuracy, even though competitive with the state of the art, remains a challenge. The primary target customers include law enforcement agencies, private security companies, and public administrations involved in smart city initiatives. The estimated time to market is three years. VICOM, as a non-profit organization, plans to integrate this result into its product portfolio. The commercialization strategy is still under elaboration.

Key Information

- TRL: Started at 4, expected to reach 6.
- Owner: VICOM (sole owner).
- Market: Law enforcement, private security, public administrations (smart city initiatives).
- Strengths: Real-time traffic event analysis.
- Challenges: Relies on supervised semantic interpretation, relatively low practical accuracy.
- Exploitation: Licensing model.
- Time to Market: 3 years.
- Potential as KER.

ER11: Traffic Anomaly Dataset

The Traffic Anomaly Dataset consists of short video clips simulating hazardous traffic situations in tunnels. The dataset was generated using the BeamNG simulation engine and includes variations of four anomalous events: traffic jams, stopped or broken vehicles, vehicle accidents, and vehicle fires. This dataset was suggested and developed by VICOM, which is also the sole owner and has no additional contributors. The related task from the Grant Agreement is T6.4. The primary purpose of this dataset is public release for research purposes, with no specific TRL level assigned. The main strength of the dataset is its ability to provide realistic simulations of hazardous traffic scenes for AI training. However, its limitations include the absence of real-world recordings and a limited number of simulated activities. The dataset contributes to public domain knowledge and does not have direct competitors. The targeted market includes public and private security agencies and research institutions. Following public dissemination activities, the dataset will be available during the project. VICOM, as a non-profit organization, plans to incorporate this dataset into its research portfolio. The final scope of supported events is still under elaboration.

Key Information

- TRL: Not applicable (public research dataset).
- Owner: VICOM (sole owner).
- Market: Public and private security agencies, research institutions.
- Strengths: Realistic traffic anomaly simulations for AI training.
- Challenges: No real-world recordings and a limited number of simulated activities.
- Exploitation: Public release for research purposes.
- Availability: During the project.
- Potential as KER.

ER12: Multi-Modal Fusion Schemes

The Multi-Modal Fusion Scheme is a software component designed to support the full integration of all data sources within the TESTUDO project into a standard and accessible format. This enables seamless bidirectional data utilization across monitoring system components. It was suggested and developed by CENTRIC, with contributions from ENG. The relevant tasks from the Grant Agreement are T8.1, T9.1, T4.2, and T5.2. The module started at TRL 4 and is projected to reach TRL 6 by the project's end. The exploitation potential is significant as many Horizon 2020 projects require multi-modal fusion for increasingly complex solutions. The scheme's main strength is integrating diverse data types into a unified format. At the same time, challenges include compatibility with other TESTUDO modules and integration with critical infrastructure (CI) internal systems. Opportunities arise from the increasing role of AI and machine learning in automating data integration and pattern recognition. However, risks include interoperability issues and a lack of internet connectivity in some CI environments. The primary competitors include BAE Systems, which develops fusion technologies for defence and infrastructure, and Palantir, which provides data fusion platforms for intelligence and security applications. The targeted market includes governmental and research organizations, SMEs, and private entities involved in CI monitoring. The expected time to market is at the end of the project. As part of Sheffield Hallam University, CENTRIC aims to incorporate this result into future research initiatives. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 6.
- Owner: CENTRIC (with contributions from ENG).
- Market: Government agencies, research organizations, SMEs, CI monitoring entities.
- Strengths: Integration of diverse data types into a unified format.
- Challenges: Compatibility with TESTUDO modules, CI system integration, and connectivity issues.
- Time to Market: End of the project.
- Potential as KER.

ER13: Threat Assessment Module

The Threat Assessment Module is a methodology for assessing the vulnerability of AI models to evasion attacks. It was suggested and developed by VICOM, the sole owner, with no additional contributors. The module is linked to task T8.2 in the Grant Agreement. The module started at TRL 4 and is expected to reach TRL 5 by the project's conclusion. The primary commercialization strategy involves licensing. The module enhances AI model security by analysing convolutional neural network (CNN) vulnerabilities. Its strength lies in its ability to optimize the analysis of deep learning models, but a challenge is the lack of extensive real-world validation. The market potential is strong due to the growing importance of cybersecurity in AI development. The targeted customers include cybersecurity firms and AI development companies. The expected time to market is to be determined. VICOM intends to integrate this result into its research portfolio, but the commercialization path is still being elaborated.

Key Information

- TRL: Started at 4, expected to reach 5.
- Owner: VICOM (sole owner).
- Market: Cybersecurity firms, AI development companies.
- Strengths: Optimizes analysis of CNN vulnerabilities.
- Challenges: Limited real-world validation.
- Exploitation: Licensing model.
- Time to Market: To be determined.
- Potential as KER.

ER14: Prediction and Simulation Models

The Prediction and Simulation Models are software components designed to forecast and simulate events for early situational awareness. CERTH, the sole owner, suggested and developed these models without additional contributors. The related tasks of the Grant Agreement are T8.3 and T9.3. The module started at TRL 4 and is projected to reach TRL 7 by the project's end. The intended exploitation pathways include internal use, further research, and future projects. The key advantage of these models is their ability to provide early awareness of critical evolution. However, their generalization remains challenging due to the low maturity of specific AI-based prediction techniques. The opportunities for this module are significant, given the increasing demand for predictive security solutions. An important risk is the lack of high-quality datasets or limited sensor coverage, which could affect prediction accuracy. The target market includes government agencies, industry partners, SMEs, and research institutions. CERTH, as a non-profit organization, aims to extend its expertise in predictive modelling and may consider spin-off opportunities. The commercialization timeline is yet to be determined.

Key Information

- TRL: Started at 4, expected to reach 7.
- Owner: CERTH (sole owner).
- Market: Government agencies, industry partners, SMEs, research institutions.
- Strengths: Provides early situational awareness.
- Challenges: Generalization issues, dependency on high-quality datasets and sensor coverage.
- Exploitation: Internal use, further research, future projects.
- Time to Market: To be determined.
- Potential as KER.

ER15: Optimized 3D Mapping Module

The Optimized 3D Mapping Module is a software tool developed by CERTH for creating virtual 3D maps from visual content. It was suggested and developed by CERTH, with no additional contributors. The relevant tasks from the Grant Agreement are T4.6 and T5.6. The module started at TRL 4 and is expected to reach TRL 6 by the project's completion. Its intended exploitation paths include internal use, further research, and integration into future projects. The primary advantage of this module is its ability to generate photorealistic 3D models of infrastructure using easily accessible visual data. However, the low maturity of the technology and the need for offline processing due to the complexity of the task pose challenges. The rise of AI and machine learning and increased interest in augmented and virtual reality present substantial market opportunities. Key risks include regulatory restrictions and insufficient funding for 3D mapping technologies. Major competitors in this space include Pix4D, ESRI, Autodesk, Adobe, Bentley, and Maxon. The target market includes architecture, engineering, construction, media, entertainment, manufacturing, safety, and security applications. The estimated time to market is between three and five years. CERTH, as a non-profit organization, intends to use this result to expand its research expertise and may explore spin-off opportunities. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 6.
- Owner: CERTH (sole owner).
- Market: Architecture, engineering, construction, media, entertainment, manufacturing, safety, and security.
- Strengths: Generates photorealistic 3D models from visual data.
- Challenges: Low maturity, requires offline processing.
- Time to Market: 3–5 years.
- Potential as KER.

ER16: Enriched Data Model Tailored for CI Protection

The Enriched Data Model, or Incident Detection Message Exchange Format version 2 (IDMEFv2), is a universal format that describes events and incidents detected in cyber and physical infrastructures. It can also document natural and man-made hazards. ENG, the sole owner, suggested and developed this result without additional contributors. The related tasks from the Grant Agreement are T4.2 and T5.2. The module has no assigned TRL but is positioned as a standard for use in research projects and as a foundation for further research and standardization efforts. The key strength of IDMEFv2 is its interoperability across diverse domains, facilitating standardized event reporting for CI operators, cybersecurity providers, and emergency response organizations. However, challenges include adoption barriers, limited applicability to specific event types, and reliance on standardization efforts. Market opportunities arise from the increasing demand for standardized incident reporting and new stakeholders in various sectors. Risks include low adoption rates and competition from alternative incident management solutions such as

Common Event Format (CEF) and Open Threat Exchange. The primary market consists of CI operators dedicated to detection activities. The format is ready for market use and will be maintained as part of ENG's standardization initiatives. It is not considered a KER.

Key Information

- TRL: Not assigned (positioned as a standard for research and standardization).
- Owner: ENG (sole owner).
- Market: CI operators, cybersecurity providers, and emergency response organizations.
- Strengths: Interoperability across domains, standardized event reporting.
- Challenges: Adoption barriers, limited applicability to specific events, reliance on standardization.
- Time to Market: Ready for use.
- Not considered a KER.

ER17: XR Technologies Components

XR Technologies Components involve a novel extended reality (XR) application deployed on a standalone XR headset to enhance situational awareness for Command and Control (C2) operators. This result was suggested and developed by CENTRIC, with contributions from CERTH. The related tasks from the Grant Agreement are T6.2, T7.2, T8.3, T9.3, T8.4, and T9.4. The module started at TRL 4 and is expected to reach TRL 6 by the project's end. The primary exploitation strategy focuses on internal use, further research, and integration into future projects. XR technologies offer increased situational awareness and a customizable user interface for enhanced operator experience. However, challenges include the low maturity of XR hardware, potential low battery life, and usability concerns. Market opportunities exist as XR headsets become commercially viable for businesses. Still, risks include the slow evolution of XR technology and the potential reluctance of CI operators to adopt it due to discomfort or unfamiliarity. The target market includes private security entities and CI monitoring organizations. The estimated time to market is by the end of the Proof of Concept 3 (PUC3). As a non-profit organization, Sheffield Hallam University intends to develop the XR application further for a broader range of XR headsets. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 6.
- Owner: CENTRIC (with contributions from CERTH).
- Market: Private security entities, CI monitoring organizations.
- Strengths: Enhances situational awareness and customizable user interface.
- Challenges: Low XR hardware maturity, battery life, usability concerns.
- Opportunities: The Growing commercial viability of XR headsets.

- Risks: Slow XR adoption and operator reluctance.
- Time to Market: End of Proof of Concept 3 (PUC3).
- Potential as KER.

ER18: Monitoring Centre for CI Protection

The TESTUDO Monitoring Centre is a comprehensive security solution that integrates data from multiple sensors and sources. It leverages AI-driven threat prediction, Digital Twins (DTs), and XR functionalities to enhance situational awareness for CI operators and security professionals. This result was suggested and developed by this STWS with contributions from CENTRIC, ENG, PIAP, DFKI, DRAXIS, ADS, and PROSEGUR. The related tasks from the Grant Agreement are T8.4 and T9.4. The module started at TRL 5 and is expected to reach TRL 7 by project completion. The centre has strong market potential due to the increasing demand for automated security solutions involving UXVs and AI-driven monitoring. Strengths include intelligent mission planning, enhanced situational awareness, and seamless integration with unmanned systems. However, challenges include operator training requirements, implementation costs, and maintenance expenses. The growing interest in robotic security solutions and existing infrastructure in security operations centres present opportunities for market adoption. Risks include market competition and potential integration challenges. The targeted market comprises critical infrastructure operators, security providers, and defence organizations. The estimated time to market is three to five years. The path to market includes pilot installations, cybersecurity analysis, legal agreements, and marketing strategies. This result is under further evaluation for KER status.

Key Information

- TRL: Started at 5, expected to reach 7.
- Owner: STWS (with contributions from CENTRIC, ENG, PIAP, DFKI, DRAXIS, ADS, PROSEGUR).
- Market: Critical infrastructure operators, security providers, and defence organizations.
- Strengths: AI-driven threat prediction, Digital Twins, XR integration, intelligent mission planning.
- Challenges: Operator training, implementation costs, maintenance expenses.
- Opportunities: There is a Growing demand for robotic security solutions and AI-driven monitoring.
- Risks: Market competition and integration challenges.
- Time to Market: 3–5 years.
- KER Status: Under evaluation.

ER19: UAVs CERBERUS and DIOPTRA Prototypes

The UAVs CERBERUS and DIOPTRA are novel aerial robotic platforms designed for over-ground surveys and enhanced autonomy, incorporating multi-sensor capabilities. ACCELL, the sole owner, suggested and

developed this result without additional contributors. The related tasks from the Grant Agreement include T3.2, T4.3, T5.3, T4.4, T5.4, T6.1, T7.1, T6.2, T7.2, T6.3, T7.3, T6.5, T7.5, T8.5, T9.5, and T10.5. The UAVs started at TRL 5 and are expected to reach TRL 7 by project completion. The primary exploitation strategy includes commercialization, internal use, further research, technical development, and service offerings. Strengths include real-time operational awareness, enhanced security monitoring, threat evaluation capabilities, and the ability to host multiple sensor payloads, including thermal, multispectral, and LIDAR. However, challenges include high data volume, training and maintenance costs, and technological maturity constraints. Opportunities exist in mass production to reduce costs and expand market reach, but potential risks include competition from larger players with better financial and technological leverage and regulatory barriers. The primary market consists of governmental security agencies, research institutions, SMEs, and private entities in CI monitoring. The estimated time to market is within two years, with an expected return on investment (ROI) of 20–30%. ACCELI plans to develop new products, refine prototypes, and pursue further research to commercialize the UAVs. This is considered a KER.

Key Information

- TRL: Started at 5, expected to reach 7.
- Owner: ACCELI (sole owner).
- Market: Government security agencies, research institutions, SMEs, CI monitoring.
- Strengths: Real-time operational awareness, multi-sensor capabilities (thermal, multispectral, LIDAR), threat evaluation.
- Challenges: High data volume, training and maintenance costs, and technological maturity constraints.
- Opportunities: Mass production for cost reduction and market expansion.
- Risks: Competition from more prominent players and regulatory barriers.
- Time to Market: 2 years.
- Expected ROI: 20–30%.
- Potential as KER.

ER20: Site Scouting UGV

The Site Scouting UGV is a lightweight (under 15kg), highly mobile, all-terrain, unmanned ground vehicle designed for autonomous or remote-controlled disaster site exploration. DFKI, the sole owner, suggested and developed this result without additional contributors. The related tasks from the Grant Agreement are T4.5, T8.5, and T10.2. The UGV started at TRL 6 and is expected to reach TRL 7 by project completion. The primary exploitation strategy includes further research, commercialization via a spin-off, or integration into DFKI's commercial branch. Strengths include proven UGV concepts with excellent all-terrain capabilities, while weaknesses involve improvements in autonomy software and hardware robustness. Market opportunities exist in disaster management, security, agriculture, and environmental

monitoring. However, challenges include system complexity, maintenance costs, and operational range limitations. Competition is increasing, particularly from aerial drones and Chinese UGV vendors. The targeted customers include government agencies, private security firms, and critical infrastructure operators. The estimated time to market is three years for a fully certified off-the-shelf product.

Key Information

- TRL: Started at 6, expected to reach 7.
- Owner: DFKI (sole owner).
- Market: Disaster management, security, agriculture, environmental monitoring.
- Strengths: Lightweight, highly mobile, all-terrain capabilities.
- Challenges: Autonomy software improvements, hardware robustness, maintenance costs.
- Opportunities: Spin-off commercialization and integration into DFKI's commercial branch.
- Risks: Competition from aerial drones and Chinese UGV vendors.
- Time to Market: 3 years.
- Potential as KER.

ER21: Situation Awareness Framework for Enhancing CI Resilience (SAFER)

SAFER is an advanced software tool integrating real-time data analysis, anomaly detection, and risk prediction to enhance CI resilience. It comprises two primary components: SAFER and a Complex Event Processing (CEP) system. ENG, the sole owner, suggested and developed this result without additional contributors. The related tasks of the Grant Agreement are T4.2 and T8.1. The framework started at TRL 4 and is expected to reach TRL 6 by project completion. The primary commercialization strategy involves direct product commercialization, licensing, and service provision. SAFER provides a holistic security solution with predictive analytics, real-time threat awareness, and decision support; however, integration complexity, cost, and adoption barriers present challenges. The target market includes CI operators, public sector agencies, and private security providers. The estimated time to market is 18–30 months, with an expected ROI of 100–200% in the first three years. ENG plans to integrate SAFER into its security offerings and adopt a subscription-based licensing model. This is considered a KER.

Key Information

- TRL: Started at 4, expected to reach 6.
- Owner: ENG (sole owner).
- Market: CI operators, public sector agencies, private security providers.
- Strengths: Predictive analytics, real-time threat awareness, and decision support.
- Challenges: Integration complexity, cost, and adoption barriers.

- Exploitation: Direct commercialization, licensing, and service provision.
- Time to Market: 18–30 months.
- Expected ROI: 100–200% in 3 years.
- Potential as KER.

Table 1 summarizes the key information from the exploitable results of TESTUDO.

ER ID	Title	Owner	TRL Start	TRL End	Market	Time to Market	KER	Strengths	Challenges
ER1	Maximized Surveillance Swarm Intelligence Module	SINTEF	4	7	Critical infrastructure, defence, search & rescue, agriculture, forestry	4 years	Yes	Planning missions to maximize surveillance efficiency	Integration with heterogeneous hardware
ER2	Autonomous Resource Allocator Module	SINTEF	4	7	Critical infrastructure, defence, search & rescue, agriculture, forestry	4 years	Yes	Dynamic matching of resource allocation to demand	Smooth integration with heterogeneous hardware
ER3	Network Infrastructure	CEA	4	7	Drone operators, critical infrastructure, defence, security organizations	4 years	Yes	Seamless integration with robotic platforms	Integration with onboard drone hardware
ER4	Visual Detection Module	CERTH	5	7	Law enforcement, first responders, critical infrastructure operators	2 years	Yes	Low complexity, high performance	Untested robustness in diverse environments
ER5	Multispectral Detection Module	CERTH	4	7	Law enforcement, first responders, critical infrastructure, security applications	3 years	Yes	High efficiency in thermal detection	Uncertain performance in untested environments
ER6	Detection Module on Embedded Platforms	TEKNIKER	5	7	Critical infrastructure, defence, search & rescue, agriculture, forestry	4 years	Yes	AI detection with low power consumption	Hardware compatibility, older neural network reliance
ER7	CBRN Detection Tools	T4i	4	7	Tunnel operators, construction, fire brigades, police, UAV providers, chemical industries, environmental agencies	3 months	Yes	Real-time detection, UAV adaptability, lightweight	Maintenance, complexity perception

ER ID	Title	Owner	TRL Start	TRL End	Market	Time to Market	KER	Strengths	Challenges
ER8	Cyber-Threat Detection Module	CEA	5	7	Critical infrastructure, network ops, defence/security sectors	4 years	Yes	Detects unknown threats vs. signature-based systems	High false positives from traffic variability
ER9	Low-Power Hardware for Machine Vision	TEKNIKER	4	7	First responders, surveillance, critical infrastructure, defence, agriculture	4 years	Yes	AI detection at low power	Limited real-world testing and integration
ER10	Visual Activity Recognition Module	VICOM	4	6	Law enforcement, private security, public admin (smart cities)	3 years	Yes	Real-time traffic event analysis	Supervised semantic reliance, low accuracy
ER11	Traffic Anomaly Dataset	VICOM	n/a	n/a	Security agencies, research institutions	During project	Yes	Realistic simulations for AI training	No real-world data, limited activities
ER12	Multi-Modal Fusion Schemes	CENTRIC (w/ ENG)	4	6	Government orgs, research, SMEs, CI monitoring	End of project	Yes	Unified data integration	TESTUDO compatibility, CI integration issues
ER13	Threat Assessment Module	VICOM	4	5	Cybersecurity firms, AI developers	TBD	Yes	Optimizes CNN vulnerability analysis	Limited real-world validation
ER14	Prediction and Simulation Models	CERTH	4	7	Government agencies, industry, SMEs, research	TBD	Yes	Early situational awareness	Low maturity of AI prediction, data needs
ER15	Optimized 3D Mapping Module	CERTH	4	6	Architecture, engineering, media, security	3 - 5 years	Yes	Photorealistic 3D models from visuals	Low maturity, offline processing
ER16	Enriched Data Model for CI	ENG	n/a	n/a	CI ops, cybersecurity, emergency responders	Ready	No	Cross-domain interoperability	Adoption, limited event types
ER17	XR Technologies Components	CENTRIC (w/ CERTH)	4	6	Private security, CI monitoring	End of PUC3	Yes	Situational awareness with XR, UI customization	Low XR maturity, usability concerns

ER ID	Title	Owner	TRL Start	TRL End	Market	Time to Market	KER	Strengths	Challenges
ER18	Monitoring Centre for CI Protection	STWS (multi-partner)	5	7	CI ops, security providers, defence	3 - 5 years	Under Evaluation	AI threat prediction, Digital Twins, mission planning	Training, cost, integration
ER19	UAVs CERBERUS and DIOPTRA	ACCELI	5	7	Government security, SMEs, CI monitoring	2 years	Yes	Real-time awareness, multi-sensor payloads	Training costs, data volume, maturity
ER20	Site Scouting UGV	DFKI	6	7	Disaster management, agriculture, environment, security	3 years	Yes	Lightweight, mobile, all-terrain	Autonomy software, robustness
ER21	SAFER - CI Resilience Framework	ENG	4	6	CI ops, public sector, private security	18 - 30 months	Yes	Predictive analytics, threat awareness	Integration complexity, adoption barriers

Table 1. Exploitable Results Overview.

3. IPR Management

Intellectual Property Rights (IPR) management is a critical component of the TESTUDO project, ensuring that all innovations, knowledge, and technological advancements generated during the project are correctly identified, protected, and utilized. As an EU-funded Horizon project, TESTUDO operates under a structured framework that balances open knowledge dissemination with the need for proprietary protection, fostering collaborative research and commercialization opportunities.

The TESTUDO project aims to develop an advanced, autonomous security framework for critical infrastructure protection using heterogeneous unmanned systems, AI-based threat prediction, and digital twins. Given the multidisciplinary nature of the consortium—which includes research institutions, technology providers, and end-user organizations—effective IPR management is essential to support knowledge sharing while safeguarding valuable assets. A robust IPR strategy ensures compliance with Horizon Europe regulations and maximizes the impact of the project’s results by enabling their exploitation in industry, academia, and policy-making.

One of the key challenges in managing IPR within a large consortium is the diverse nature of knowledge contributions. Some partners bring pre-existing intellectual assets into the project (Background Knowledge), while innovations emerge as part of the research and development process (Foreground Knowledge). Additionally, the TESTUDO project may generate Sideground Knowledge—new insights that are not directly linked to the project’s core objectives but are valuable for future applications. To address these complexities, the consortium follows structured ownership and access rights agreements, ensuring all parties can benefit from the project results according to their contribution level.

IPR protection in TESTUDO encompasses multiple mechanisms, including patents, copyright, trade secrets, licensing agreements, and open-access publishing where applicable. The project follows the principles of the Horizon Europe Model Grant Agreement, which stipulates clear rules on ownership, access rights, and exploitation of results. The consortium agreement further defines each partner's specific roles and obligations with intellectual property, facilitating a transparent and legally sound collaboration.

Furthermore, TESTUDO’s IPR strategy's key objective is to ensure that the knowledge and technological advancements generated within the project are effectively exploited beyond the project’s lifetime. This includes potential commercialization pathways such as licensing agreements, spin-off companies, and strategic partnerships with industry stakeholders. The IPR management approach also aligns with the European Commission’s Open Science and Open Innovation policies, ensuring that publicly funded research contributes to scientific progress while respecting commercial interests.

3.1. Types of Knowledge

The knowledge generated within the TESTUDO project can be classified into four main categories: Foreground Knowledge, Background Knowledge, Sideground Knowledge, and Open Knowledge. These classifications ensure that intellectual property (IP) is appropriately managed, shared, and exploited while protecting proprietary information.

1. Foreground Knowledge

Foreground Knowledge refers to new knowledge, results, and innovations generated during the execution of the TESTUDO project. This includes:

- Technical advancements include software algorithms, AI-based models, cybersecurity tools, and surveillance solutions.
- Prototypes and demonstrators developed for infrastructure protection, including UAVs, UGVs, and digital twin simulations.
- Methodologies and frameworks for threat prediction, incident response, and multi-modal data fusion.
- New datasets created from project activities, including sensor data, video analytics, and cyber threat intelligence.

Key Features of Foreground Knowledge:

- Owned by the partner(s) that generated it.
- Joint ownership applies when multiple partners contribute to a single result.
- Subject to access rights for other partners as per the Grant Agreement.
- Can be protected through patents, copyrights, and trade secrets.

Example Foreground Knowledge from TESTUDO:

- **Swarm Intelligence Module:** An advanced AI-driven system for coordinating UAVs in infrastructure surveillance, developed by SINTEF as part of T4.4 and T5.4. This module is classified as Foreground Knowledge because it is a novel project outcome, not pre-existing knowledge..
- **Cyber-Threat Detection Model:** A real-time anomaly-based intrusion detection system (IDS) developed by CEA under T6.6. This qualifies as Foreground Knowledge, an innovation created within TESTUDO, extending beyond pre-existing cybersecurity models.
- **Visual Activity Recognition Module:** An AI-driven software component that detects suspicious activities in critical infrastructure areas, developed under T6.3 and T7.3 by TEKNIKER. It is considered Foreground Knowledge as it results from project research and is intended for further exploitation.

2. Background Knowledge

Background Knowledge consists of pre-existing knowledge and technologies that consortium partners bring into the project. This includes:

- Patented or proprietary technologies, software, and methodologies developed before the project.
- Existing data models, analytics tools, or security frameworks.
- Trade secrets, expertise, and know-how relevant to the project's objectives.

Key Features of Background Knowledge:

- Remains the property of the original owner.
- Access rights must be granted to other consortium members when necessary for project execution.
- To be defined in the Consortium Agreement to avoid conflicts over proprietary technologies.

Example Background Knowledge:

- Existing AI Models for Image Recognition (provided by a partner research institution).
- Cybersecurity Monitoring Software (already developed by a commercial partner).
- GIS-Based Critical Infrastructure Mapping Tools (brought by a partner specializing in geographical information systems).

3. Sideground Knowledge

Sideground Knowledge includes new findings that emerge during the project but are not directly related to its core objectives. While not essential for TESTUDO's main deliverables, this knowledge can offer value in other research, commercial, or technological applications.

Key Features of Sideground Knowledge:

- Generated within the project but not planned as a key outcome as part of the broader knowledge management and IP strategy outlined in the Grant Agreement.
- Owned by the partner(s) that developed it.
- Can be exploited outside the scope of TESTUDO after project completion unless restrictions apply due to strategic assets, security considerations, or prior agreements requiring approval for third-party transfers, as the Grant Agreement outlines.

Example Sideground Knowledge:

- New optimization algorithms have been developed for UAV path planning that can be applied in logistics or transportation.
- Advancements in Battery Efficiency for autonomous ground vehicles could be helpful to for electric vehicle applications.
- Human-Machine Interface (HMI) Improvements for real-time monitoring systems, potentially beneficial in smart city applications.

4. Open Knowledge

Open Knowledge refers to research outputs and results intended for public dissemination. This aligns with the Horizon Europe Open Science Policy, which encourages the sharing of research findings to maximize societal impact.

Key Features of Open Knowledge:

- Includes publicly available datasets, open-access publications, and non-commercial software.
- Encourages transparency, collaboration, and broader adoption of research outcomes.
- Must comply with EU regulations such as GDPR for handling sensitive data (as outlined in Article 5 and Article 89(1) GDPR, ensuring lawful processing, data minimization, and strict confidentiality requirements as stated in the Grant Agreement).

Example Open Knowledge from TESTUDO:

- Public Dataset of Threat Scenarios for training AI security models.
- Research Papers on AI-based surveillance Methods published in open-access journals.
- Open-Source Software Components for cyber threat detection.

3.2. Record of Intellectual Property Assets

Proper management and documentation of IP assets are essential for ensuring that the knowledge, innovations, and technological advancements generated in TESTUDO are adequately protected, utilized, and exploited. A well-maintained Record of IP Assets helps establish ownership, prevent disputes, and facilitate commercialization and dissemination in compliance with Horizon Europe regulations.

The TESTUDO project, which focuses on autonomous security solutions for critical infrastructure protection, involves multiple research institutions, technology developers, and end-users and generates a broad range of IP assets. These assets include patents, copyrights, trade secrets, trademarks, software, datasets, and methodologies. The record-keeping system ensures these assets are classified, documented, and accessible to relevant stakeholders under controlled conditions.

The section outlines the types of IP assets generated, their ownership, protection mechanisms, and exploitation strategies to maximize their impact while safeguarding proprietary rights.

Classification of Intellectual Property Assets

Intellectual Property assets in TESTUDO can be categorized into the following groups:

- 1. Patents and Patent Applications**—Patents protect novel inventions such as AI-driven threat detection, autonomous vehicle systems, and advanced sensor fusion techniques. They are filed to grant exclusive rights and prevent unauthorized use.
- 2. Copyright-Protected Materials** – Covering original works including software, documentation, training materials, and research publications. This ensures proper attribution and licensing control over project outputs.

3. **Trade Secrets and Confidential Know-How** – Proprietary methodologies, algorithms, and undisclosed techniques developed within TESTUDO that require confidentiality measures like NDAs and restricted access.
4. **Trademarks and Branding Elements** – Project logos, brand names, and visual identity elements that differentiate TESTUDO's innovations in the market and support commercialization efforts.
5. **Data and Datasets**—Large-scale datasets generated from project activities, including sensor data from UAVs, cyber threat intelligence logs, and infrastructure monitoring data, are all managed under strict data governance policies.

Intellectual Property Recording and Management System

To maintain transparency and compliance, the TESTUDO consortium follows a structured approach to IP documentation:

1. **IP Registry** – A centralized database recording each IP asset's description, ownership, protection status, and exploitation strategy.
2. **Access and Ownership Policies** – Clearly define foreground knowledge ownership by the generating partner, joint ownership rules, background knowledge access rights, and conditions for knowledge sharing among partners.
3. **3. Exploitation Pathways** – Ensuring IP assets are leveraged through licensing agreements, open-source releases where applicable, collaboration with industry for technology transfer, and potential spin-off companies.

3.3. Ownership Schemas

Intellectual property ownership within the TESTUDO project is critical to ensuring fair rights distribution, proper utilization of innovations, and effective exploitation of project results. Given the collaborative nature of the consortium, where multiple partners contribute to research, development, and implementation, ownership schemas must be clearly defined to avoid conflicts and maximize the impact of the project's outcomes.

The ownership structure is governed by the Horizon Europe Grant Agreement and further refined in the Consortium Agreement. These agreements ensure compliance with EU regulations while accommodating each partner's specific needs and contributions. They set the legal framework for determining ownership rights, assigning access rights, and defining conditions for protecting and exploiting knowledge generated within the project.

Ownership of Foreground Knowledge

Foreground Knowledge refers to any new results, including inventions, software, methodologies, and datasets, generated during the TESTUDO project. The default principle established in Horizon Europe states that ownership belongs to the partner(s) responsible for generating the specific result. If multiple partners contribute to creating an innovation, joint ownership applies unless otherwise agreed.

In cases of joint ownership, each contributing partner has an equal right to use and exploit the results, provided that they consult with co-owners, ensure fair financial arrangements, and respect confidentiality obligations. If one partner wishes to license or transfer a jointly owned result to a third party, all co-owners must obtain explicit consent, unless a separate agreement has been made in advance.

To facilitate exploitation and commercialization, joint ownership agreements may include provisions for exclusive exploitation by one partner, subject to financial compensation or licensing arrangements for the co-owners. Such agreements must be documented and aligned with the Consortium Agreement to ensure clarity and fairness.

Ownership of Background Knowledge

Background Knowledge consists of pre-existing technologies, methodologies, patents, software, and expertise that consortium members bring into the project. Each partner retains full ownership of their Background Knowledge, and no transfer of ownership occurs due to participation in TESTUDO. However, Background Knowledge may be made available to other consortium members under predefined access rights, either royalty-free or under fair and reasonable conditions.

If a partner needs access to another consortium member's Background Knowledge to execute project tasks or further exploit Foreground Knowledge, the terms of access must be established in writing. The Consortium Agreement outlines these terms, ensuring that Background Knowledge is shared in a controlled manner while protecting the intellectual property rights of the owning partner.

Transfer of Ownership

The TESTUDO Grant Agreement allows for transferring ownership of Foreground Knowledge under specific conditions. If a partner wishes to transfer ownership of an innovation or technological result, they must notify the other consortium members in advance. This ensures that all stakeholders can assess the impact of the transfer, mainly if the knowledge in question is critical to the project's objectives or future exploitation.

Transfers of ownership may occur in various contexts, including:

- **Commercialization efforts**, where a partner seeks to license or sell a technology to an external company.
- **Spin-off creation**, where new business entities are formed to develop further and commercialize TESTUDO results.
- **Mergers or acquisitions**, where a partner undergoes corporate restructuring and ownership of IP assets changes as part of the process.

When transferring ownership, the new owner must accept the obligations established in the Grant Agreement, particularly regarding access rights and exploitation commitments. Any partner affected by a transfer of ownership may request continued access rights if necessary to implement the project or to use the results further.

Access Rights for Consortium Members

To ensure collaboration and maximize the impact of project results, the Consortium Agreement defines specific access rights that partners have to each other's knowledge. These access rights enable members to use Background and Foreground Knowledge in ways that support both project execution and post-project exploitation.

During the project, all partners are granted access rights to necessary Background and Foreground Knowledge on a royalty-free basis, provided such access is essential for fulfilling project tasks. Access rights may be extended after the project's conclusion to facilitate commercialization, further research, or industrial applications. However, these rights must be negotiated and agreed upon in advance.

Suppose a partner withdraws from the project or ceases participation. In that case, they must ensure that any knowledge they have contributed remains accessible to the remaining consortium members as per the agreed access rights. This prevents disruptions in project continuity and guarantees that key knowledge remains exploitable by the TESTUDO consortium.

Ownership and Exploitation of Joint Results

In cases where multiple partners contribute to a single innovation or technological development, a joint ownership agreement is established to define the terms of use, licensing, and revenue sharing. These agreements ensure that all contributing partners can benefit from the results, while also allowing for streamlined exploitation and commercialization.

Joint ownership agreements typically cover:

- **The proportion of ownership for each partner**, based on their contribution level.
- **The process for licensing the jointly owned result** to third parties.
- **Conditions for using the result internally** within each organization.
- **Revenue-sharing mechanisms** if commercialization generates financial returns.

If no formal agreement is reached, default Horizon Europe rules apply, granting each co-owner an equal share of the result, with the right to independently exploit it while ensuring fair compensation to the other owners.

Dispute Resolution and Governance

The TESTUDO consortium follows a structured dispute resolution process to prevent ownership disputes. If disagreements arise over ownership rights, access rights, or exploitation terms, the issue is first addressed through internal discussions among the affected partners. Mediation or arbitration mechanisms outlined in the Consortium Agreement may be invoked if no resolution is reached.

Ownership-related matters are managed by the project's IPR Management Committee, which includes representatives from key partners. This committee is responsible for:

- Reviewing ownership claims and resolving disputes.
- Ensuring compliance with IP protection mechanisms.

- Advising on best practices for knowledge transfer and commercialization.

By establishing clear governance structures, the consortium ensures that IP-related decisions are handled transparently and aligned with the TESTUDO project's strategic objectives.

3.4. IPR Matrix

The TESTUDO project's IPR Matrix serves as a structured framework for defining ownership, access rights, protection mechanisms, and exploitation routes for different IP assets. Given the project's multidisciplinary and multi-partner nature, ensuring a clear, well-defined IPR strategy is essential for maximizing impact, avoiding conflicts, and facilitating commercialization.

The IPR Matrix categorizes intellectual property assets into key types, specifies ownership models, and outlines the conditions under which these assets can be accessed, used, and exploited by consortium members, third parties, and commercial entities. The TESTUDO Consortium Agreement and Grant Agreement provide the legal basis for applying this matrix, ensuring compliance with Horizon Europe regulations and best practices in research collaboration.

The matrix is designed to balance the need for collaboration, knowledge sharing, and open science with the necessity of protecting proprietary innovations, enabling commercialization, and ensuring a return on investment for project partners. Below, we detail the various elements of the IPR Matrix.

The IPR Matrix is structured based on key categories of intellectual property within TESTUDO, including:

- **Type of IP Asset**
- **Ownership**
- **Access Rights**
- **Protection Mechanisms**
- **Exploitation Route**

Each of these elements ensures that intellectual property is managed effectively, avoiding ambiguity and securing the interests of both generating partners and users.

Type of IP Asset

Intellectual property within TESTUDO can be classified into distinct categories, each requiring different handling in terms of protection and exploitation.

- 1. Patents and Patent Applications** – Protecting technical innovations such as AI algorithms, surveillance methodologies, cybersecurity systems, and unmanned aerial/ground vehicle solutions.
- 2. Copyright-Protected Software and Code** – Covering AI-driven security software, digital twins, and data analytics platforms.
- 3. Trade Secrets and Confidential Know-How** – Proprietary algorithms, methodologies, and processes developed within the project.

4. **Trademarks and Branding Elements** – Protecting the TESTUDO project’s brand identity, including software names and system logos.
5. **Data and Datasets**—including sensor data from UAVs, cybersecurity threat intelligence logs, and AI training datasets.
6. **Scientific Publications and Reports** – Research papers, white papers, and policy recommendations that disseminate project results.

Each category follows specific ownership and protection guidelines to ensure that the intellectual assets generated within TESTUDO are effectively utilized, commercialized, or made available to the scientific community under controlled conditions.

Ownership of IP Assets

Ownership of intellectual property in TESTUDO follows the principles established in the Horizon Europe Grant Agreement and Consortium Agreement:

- **Foreground Knowledge** is owned by the partner(s) who generate it. If multiple partners contribute, joint ownership applies.
- **Background Knowledge** remains the property of the partner who brings it into the project, with predefined access rights for other partners.
- **Sideground Knowledge**, which emerges as a by-product of the project but is not directly linked to its objectives, remains the property of the developing partner.
- **Joint Ownership Agreements** must be established where multiple partners contribute to an innovation.

For joint ownership, unless otherwise agreed, each co-owner can use the result independently, provided that fair compensation is arranged for the other co-owners.

Access Rights and Usage Conditions

Access rights define the conditions for partners to use Background and Foreground Knowledge for project-related tasks and post-project exploitation.

During the Project

- Partners are granted access rights to necessary **Background Knowledge** on a **royalty-free basis**, provided it is essential for project execution.
- **Foreground Knowledge** developed by one partner may be available to other partners under fair and reasonable conditions.
- Jointly developed results must be accessible to all contributing partners for project implementation.

After the Project

- Access rights to **Foreground Knowledge** for further research are typically provided royalty-free.

- Commercial exploitation by other consortium members requires negotiated licensing agreements.
- Access to Background Knowledge for commercial purposes may be granted under fair, reasonable, and non-discriminatory (FRAND) conditions.

These provisions ensure that project results can be used for **further development, commercialization, and scientific progress**, while protecting the proprietary interests of the generating partners.

Protection Mechanisms

Each intellectual property asset is protected using mechanisms appropriate to its category, safeguarding TESTUDO results while maintaining compliance with Horizon Europe Open Science Policies. These mechanisms allow TESTUDO partners to retain control over innovations, prevent unauthorized use, and enable structured exploitation.

1. **Patents:** Innovations with strong commercial potential are protected through patent applications, ensuring exclusive rights for their owners.
2. **Copyright:** Software, technical documentation, and research reports are automatically protected under copyright law.
3. **Trade Secrets:** Proprietary algorithms, methodologies, and confidential innovations are protected through non-disclosure agreements (NDAs) and restricted access.
4. **Trademarks:** The TESTUDO brand and associated products are safeguarded to prevent misuse or unauthorized commercialization.
5. **Data Protection:** Sensitive datasets are managed according to GDPR and FAIR data principles, ensuring responsible data governance.

Exploitation Routes

To maximize impact, TESTUDO's intellectual property assets follow structured exploitation routes:

1. **Commercial Licensing:** Patents, software, and datasets with commercial applications can be licensed to industry partners.
2. **Open-Source Release:** Selected software tools and AI models may be open-source under controlled licenses.
3. **Technology Transfer:** Innovations can be deployed to industry partners or government agencies.
4. **Spin-Off Companies:** Creating spin-offs or start-ups may further develop high-impact results.
5. **Scientific Dissemination:** Research findings are published in **open-access journals**, presented at conferences, and incorporated into policy recommendations.

Summary Table of IPR Matrix

The following matrix provides a structured overview of how TESTUDO manages its intellectual property assets:

IP Asset Type	Ownership	Access Rights	Protection Mechanisms	Exploitation Route
Patents	Generating partner(s)	Negotiable (FRAND or exclusive license)	Patent application	Licensing, Commercialization
Software (Proprietary)	Generating partner(s)	Restricted access (negotiable licensing)	Copyright, DRM	SaaS, Proprietary Licensing
Software (Open-Source)	Generating partner(s)	Open access (under specified license)	Copyright, Open-Source License	Free dissemination, industry adoption
Datasets	Generating partner(s)	Controlled access (GDPR compliance)	Data Governance Policies	AI Model Training, Research
Algorithms	Generating partner(s)	Restricted (internal use or license)	Copyright, Trade Secret	Embedded in security tools
Trademarks	Consortium or partner	Limited use (subject to agreement)	Trademark Registration	Brand Recognition, Commercial Deployment

Table 2. IPR Matrix.

3.5. Instruments for Project Results Protection

Protecting project results in TESTUDO is essential to safeguarding the innovations, methodologies, and technologies developed during the project. Given the complexity of the consortium and the involvement of multiple research institutions, technology providers, and industry stakeholders, a structured IPR protection framework is in place to ensure that all intellectual assets are adequately secured, preventing unauthorized use while facilitating controlled exploitation.

The TESTUDO project generates technological advancements in critical infrastructure security, AI-driven surveillance, cyber threat detection, and autonomous systems. If not properly protected, these results could be subject to misappropriation, limiting their commercial viability or creating security risks. The project adopts a combination of legal, technical, and procedural instruments to secure intellectual property, maintain compliance with Horizon Europe guidelines, and create a framework for sustainable exploitation.

Legal Instruments for Project Results Protection

Legal mechanisms define ownership, usage rights, and access conditions. These include patent protection, copyright laws, trademark registration, trade secret policies, licensing agreements, and contractual obligations.

Patents protect novel technological innovations, ensuring exclusive rights to the inventors and preventing unauthorized replication. The patent filing process begins with assessing patentability, followed by formal applications to relevant patent offices, securing ownership for project-generated inventions. In cases where multiple partners contribute to an invention, joint patent applications may be filed, with co-ownership arrangements ensuring equitable rights and financial returns.

Copyright is automatically granted to protect software, research publications, training materials, and digital content created in the project. This ensures that project-generated materials cannot be copied or used without appropriate permissions. Software developed within the project may be subject to copyright licenses, determining whether it will be open-source or commercialized under proprietary terms.

Trademarks protect project branding, including the names of software solutions, methodologies, and unique tools developed within TESTUDO. Registering trademarks ensures exclusivity and prevents misrepresentation or misuse by external entities. This is particularly relevant for software solutions and commercialized project outcomes.

Trade secrets cover confidential project methodologies, algorithms, and technical know-how that are not disclosed publicly. To maintain secrecy, strict Non-Disclosure Agreements (NDAs) are in place for all consortium members and external collaborators, ensuring that proprietary knowledge is shared only under controlled conditions.

Licensing agreements provide a structured framework for controlling access to project results. They specify terms under which partners, third parties, or commercial entities may use TESTUDO innovations. Depending on the consortium's strategic interests, licensing may be granted on exclusive, non-exclusive, or fair, reasonable, and non-discriminatory (FRAND) terms.

The Consortium Agreement and Grant Agreement serve as overarching legal frameworks that define intellectual property ownership, access rights, and each partner's obligations regarding project results. These agreements ensure compliance with Horizon Europe regulations and prevent disputes over intellectual property.

Technical Instruments for Project Results Protection

Technical measures play a crucial role in ensuring the security and integrity of project results. In the case of software, encryption, digital signatures, and access controls are implemented to prevent unauthorized modifications or distribution. Proprietary algorithms and AI models developed in TESTUDO are embedded with security layers to prevent reverse engineering.

Data protection mechanisms ensure compliance with GDPR and FAIR data principles for project datasets. Secure repositories, access control measures, and data anonymization techniques protect sensitive information, particularly where cybersecurity and surveillance data are involved.

Software protection strategies include code obfuscation, digital rights management (DRM), and watermarking techniques, ensuring that proprietary software cannot be altered, copied, or redistributed without authorization. When software is released as open-source, licenses such as GNU GPL, Apache, or MIT define how the code can be used, modified, and shared.

Prototypes developed within the project, including autonomous security drones, digital twin models, and AI-driven surveillance tools, are physically and digitally secured to prevent duplication. Hardware-based security measures, including firmware encryption and access authentication, ensure that deployed prototypes are protected from tampering.

Procedural and Organizational Instruments

Internal governance mechanisms ensure all partners follow IP protection and result management practices. The IPR Management Committee oversees intellectual property asset identification, documentation, and protection. Regular IP audits review innovations and determine whether they require patent filing, copyright registration, or other protective measures.

Consortium members are provided training sessions and awareness programs on intellectual property management, cybersecurity best practices, and commercialization strategies. Ensuring that all participants know their rights and obligations minimizes the risk of IP mismanagement.

A structured publication and dissemination policy regulates how project results can be shared in conferences, journals, and public forums. Before publication, an internal review process ensures that sensitive information is not disclosed prematurely, particularly for results with commercial potential or security implications.

Post-Project Protection and Exploitation Strategies

To maintain long-term protection of results beyond the project's duration, post-project exploitation agreements define how partners can continue to use and develop innovations. These agreements cover ownership retention, technology licensing, and future commercialization strategies. Where applicable, results with high commercial potential may be transferred to industry partners or startups through technology transfer agreements, ensuring controlled adoption while securing financial returns for the originating partners. Legal monitoring mechanisms track the use of project results in the market to prevent unauthorized replication. If infringement is detected, appropriate legal action can be taken to enforce TESTUDO's intellectual property rights.

3.6. Management of Knowledge

Effective knowledge management in the TESTUDO project ensures that the research outputs, technological advancements, and intellectual property generated during the project are correctly documented, protected, shared, and exploited. Given the collaborative nature of the project, which involves multiple research institutions, industry partners, and technology providers, knowledge management plays a critical role in facilitating cooperation, avoiding duplication of effort, and maximizing the impact of results.

Knowledge management in TESTUDO is structured around identifying, classifying, storing, accessing, disseminating, and exploiting information. The process involves defining clear responsibilities for partners, implementing tools and frameworks for knowledge sharing, and aligning knowledge utilization with the objectives of Horizon Europe. A structured approach ensures that foreground and background knowledge is managed effectively, allowing partners to leverage the results for further research, commercialization, and policy development.

Classification and Documentation of Knowledge

The TESTUDO project generates various forms of knowledge, including scientific discoveries, technological innovations, methodologies, data, and software tools. To manage these assets effectively, knowledge is

classified into the foreground, background, and side ground expertise, each handled according to predefined rules on ownership and access rights.

Foreground knowledge refers to new insights, technologies, and solutions developed during the project. It is systematically documented in project reports, technical papers, software repositories, and patent applications. Background knowledge includes pre-existing expertise, methodologies, and intellectual property that partners bring into the project. This knowledge remains the original owner's property but is shared under agreed conditions to support project objectives. Sideground knowledge consists of new findings that arise from the project but are not directly linked to its core deliverables. These insights may still be valuable for future research and commercial applications.

A structured knowledge recording system is in place to document all forms of knowledge, ensuring that they are accessible, retrievable, and properly categorized. This includes maintaining a centralized database of project outputs, indexing reports, and publications, and tracking the development of exploitable results. Each partner is responsible for contributing relevant knowledge to the shared repository, ensuring that all consortium members can benefit from the collective expertise.

Knowledge Sharing and Access Management

Ensuring that knowledge is accessible to the right stakeholders while maintaining protection against unauthorized use is a core aspect of knowledge management in TESTUDO. The project follows a tiered approach to knowledge access, where different levels of information availability are defined based on the sensitivity and intended use of each knowledge asset.

Internal knowledge sharing within the consortium is facilitated through dedicated collaboration platforms, data repositories, and secure communication channels. Regular meetings, workshops, and knowledge exchange sessions ensure that partners are aligned on project developments and can contribute insights to the evolving research agenda. Access rights are granted based on project needs, with clear agreements defining how other partners can use foreground and background knowledge.

External knowledge sharing follows a controlled dissemination strategy, balancing open science principles with the need to protect intellectual property. Scientific findings are published in peer-reviewed journals, presented at conferences, and made available through open-access platforms where appropriate. Software tools and datasets may be shared under specified licenses, either as open-source resources or under restricted access conditions for commercialization. In cases where knowledge has commercial value, licensing agreements are established to regulate its use by external entities.

Preservation and Security of Knowledge

Long-term preservation of knowledge is a key priority to ensure that TESTUDO's research outputs remain valuable beyond the project's duration. Secure archiving mechanisms are in place to store project documentation, source code, experimental data, and technical findings. Digital repositories maintain structured records of project deliverables, ensuring they can be retrieved and utilized.

Security measures are implemented to protect sensitive knowledge from unauthorized access or misuse. Confidential information is stored in protected environments with controlled access rights, ensuring

compliance with GDPR and other relevant data protection regulations. Encryption, authentication protocols, and data access logs are used to safeguard proprietary information, particularly in cases involving cybersecurity research and AI-driven security solutions.

Regular audits review how knowledge is managed and accessed within the project to ensure compliance with knowledge protection policies. This process helps identify potential risks, enforce data governance policies, and ensure all partners adhere to the agreed-upon knowledge-sharing frameworks.

Exploitation and Utilization of Knowledge

One of the primary goals of knowledge management in TESTUDO is to facilitate the effective exploitation of project results. This involves ensuring that knowledge generated during the project is translated into practical applications, commercial opportunities, and further research initiatives.

Industry partners involved in TESTUDO can use the knowledge developed in the project to enhance their products, integrate innovative solutions into existing systems, and create new business models. Research institutions can leverage project findings to initiate follow-up studies, secure additional funding for related research, and contribute to policy recommendations. Public authorities and policymakers may use the knowledge generated in TESTUDO to improve security strategies, regulatory frameworks, and best practices for protecting critical infrastructure.

Clear guidelines are established to support exploitation for licensing intellectual property, transferring technology to industry partners, and enabling start-ups or spin-offs based on project results. A knowledge valorisation strategy ensures that key findings are identified early, assessed for commercial potential, and supported with legal and financial mechanisms to bring them to market.

The impact of knowledge utilization is tracked through post-project monitoring efforts, evaluating how TESTUDO's results contribute to industry advancements, scientific progress, and policy developments. By maintaining strong links between knowledge producers and end-users, the project ensures that its outputs continue to generate value well beyond the initial research phase.

3.7. Project Results Protection

Protecting project results in the TESTUDO project is essential for safeguarding intellectual property, ensuring compliance with Horizon Europe regulations, and facilitating the controlled dissemination and exploitation of innovations. Given the collaborative nature of the consortium, which includes research institutions, technology providers, and industry partners, a structured protection framework is in place to secure project-generated knowledge while allowing for responsible knowledge sharing and commercialization.

Protecting project results encompasses legal, technical, and procedural measures that ensure ownership rights are respected, sensitive data is secured, and intellectual property is effectively managed. These protection mechanisms balance the need for innovation dissemination with the requirement to maintain competitive advantages and prevent unauthorized use. The TESTUDO consortium follows a strategic approach to intellectual property management, aligning protection strategies with the nature of project results, their commercial potential, and regulatory considerations.

Legal Protection of Project Results

Legal mechanisms form the foundation of project results protection in TESTUDO. These measures include patents, copyrights, trade secrets, trademarks, and licensing agreements, all of which define ownership, usage rights, and access conditions for project-generated knowledge.

Patents are used to secure exclusive rights to technological advancements developed within TESTUDO. Innovations related to AI-driven security solutions, autonomous surveillance systems, cybersecurity frameworks, and sensor technologies can be patented to prevent unauthorized replication. The patenting process involves identifying protectable results, filing applications with relevant intellectual property offices, and securing exclusive commercialization rights for the generating partner or consortium.

Copyright protection is applied to software, research publications, datasets, and training materials created in the project. This ensures that original works remain under the control of their creators and cannot be copied, modified, or distributed without permission. Software developed in the project may be protected under proprietary licenses or made available under controlled open-source models, defining how it can be used, modified, or integrated into other systems.

Trade secrets protect proprietary methodologies, algorithms, and technical knowledge that require confidentiality. Critical security-related technologies developed in TESTUDO are safeguarded through confidentiality agreements, non-disclosure agreements (NDAs), and internal access control policies to prevent unauthorized disclosure or external exploitation.

Trademarks protect the branding of project-related software tools and methodologies, ensuring that the names, logos, and visual identities associated with TESTUDO remain exclusively linked to the project. Trademark registration prevents misuse and allows for controlled commercialization.

Licensing agreements govern how third parties can access and use project results. These agreements define conditions for technology transfer, commercialization, and research collaboration. TESTUDO partners establish licensing models that enable controlled knowledge dissemination while ensuring financial returns and compliance with legal obligations.

Technical Measures for Protecting Project Results

Beyond legal instruments, technical measures are critical in ensuring project results are secure from unauthorized access, cyber threats, and intellectual property theft. These measures include encryption, digital rights management (DRM), access control systems, and cybersecurity protocols.

Encryption is implemented in software tools, datasets, and proprietary methodologies to protect against unauthorized access. Sensitive research data, particularly related to cybersecurity and AI-driven threat detection, is stored in encrypted formats to prevent breaches or leaks. Digital rights management systems control how copyrighted software and documents are accessed, modified, or distributed, ensuring compliance with intellectual property policies.

Access control mechanisms are enforced through secure data repositories and restricted database access. Only authorized consortium members and approved external users can retrieve protected information,

reducing the risk of data leaks or misuse. Strict authentication processes, including multi-factor authentication, ensure that only accredited personnel can access critical project resources.

Cybersecurity measures are applied to project-developed software, cloud-based data storage systems, and connected infrastructure to prevent unauthorized access, hacking attempts, and data manipulation. As the TESTUDO project involves research on AI-driven security solutions, protecting project results from cyber threats is critical to maintaining the integrity of the developed technologies.

Secure deployment protocols ensure that project innovations cannot be reverse-engineered or replicated without authorization for prototypes and physical assets developed within the project. Physical security measures, such as controlled access to testing facilities and secure storage of prototypes, prevent unauthorized examination or duplication of project outputs.

Procedural and Governance Approaches for Protection

Effective governance structures are crucial to protecting project results in TESTUDO. An Intellectual Property Rights Management Committee reviews intellectual property claims, ensures compliance with protection policies, and resolves potential conflicts between partners. This committee oversees the classification of knowledge, ensuring that protectable results are identified early and safeguarded accordingly.

Regular IPR audits are conducted to track the development and usage of intellectual property within the project. These audits assess whether innovations should be protected through patents, copyrights, or trade secret mechanisms and ensure that all partners comply with protection policies outlined in the Consortium Agreement.


Training programs and awareness initiatives educate project partners on intellectual property rights, cybersecurity best practices, and commercial exploitation strategies. By ensuring that all consortium members understand their responsibilities in protecting project results, the project minimizes the risk of intellectual property mismanagement.

Dissemination policies regulate how project findings are shared with the wider scientific community and industry. Before any research output is published in journals, presented at conferences, or shared in external communications, an internal review process ensures that sensitive knowledge is not prematurely disclosed. Controlled dissemination strategies prevent unauthorized use while allowing for strategic knowledge sharing.

Long-Term Protection and Post-Project Security

Ensuring that project results remain protected beyond the official duration of the project is an integral part of the TESTUDO knowledge management strategy. Post-project intellectual property agreements define how partners can continue using and commercializing project outputs while maintaining protection mechanisms.

Long-term technology transfer agreements ensure that innovations with significant commercial potential are developed further while maintaining controlled usage conditions. Some results may be transferred to



industry partners or research institutions under licensing frameworks that enable further development while retaining the intellectual property rights of the originating partner.

Monitoring and enforcement mechanisms help detect potential intellectual property infringements or unauthorized use of project results after the project has ended. Consortium members can take legal action to enforce their rights and prevent unapproved commercialization or distribution if misuse is identified.

Data retention policies ensure that sensitive research data, AI models, and technical reports remain securely stored in designated repositories. Secure archiving mechanisms allow authorized partners to continue access while preventing unauthorized modifications or distribution.

4. Preliminary Market and Competition Analysis

4.1. Business Environment

The project aims to harness cutting-edge technologies in detection, prevention, and forecasting to create an advanced platform for ongoing monitoring of Critical Infrastructure, even in challenging and distant environments.

TESTUDO is committed to a comprehensive and self-reliant security strategy for CI protection, which is in line with the European Commission's goals. Its objective is to bolster the surveillance of Europe's CI through autonomous systems and sophisticated technologies, ensuring their dependable, sturdy, and uninterrupted operation.

The project's success will be marked by achieving these operational goals:

- Providing autonomous surveillance via synergic operation of unmanned vehicles and fixed resources.
- Delivering secure and efficient telecom networks for remote areas and interoperable devices.
- Developing improved AI-based cognitive models for optimal surveillance.
- Incorporating intelligence for prediction and coordinated response.
- Ensuring increased situational awareness via novel HMI technologies.
- Validating the proposed solution via large-scale and cross-sectorial demonstrators.
- Enabling a wider deployment of robotic technologies within the European community in the CI protection domain.

Potential customers of TESTUDO solution are consortium partners, EU agencies, national governments, policymakers/agencies, industry security market operators and IT providers/Technical innovators with the highest innovation potential, investment capabilities, and needs aligned with the developed technologies.

4.2. Benefits to the Industry, Market Players, and to the Economy

The emergence of pilot technologies is poised to improve the CI sectors, influencing market players to adopt novel practices incorporating innovation and technology across their operations. Implementing the proposed technologies can undeniably enhance safety and enable more accurate data collection, reducing costs and increasing autonomy.

The consortium partners provided their input concerning what they consider:

- to be potentially beneficial to the economy from the adoption of their innovation and/or technology development;
- who will gain from utilizing this technology and how this benefit manifest; and
- how will these technologies bring about substantial – beneficial changes to their respective markets/industries?

Summarising, some of the key benefits for utilizing TESTUDO technologies include:

- Replacing the need for human inspections with personal inspections. Routine maintenance can be monitored remotely in real-time, providing instant feedback on the scenery. As a result, costs will be reduced, and the overall process will be more efficient. The risk to human life will also be decreased during essential maintenance.
- Enabling UAVs and UGVs to inspect and assess hazards before human intervention, providing a holistic overview of incidents and collecting critical data using thermal/visual cameras and other sensors.
- Allowing UAVs and UGVs to be operated by a single person without extensive safety equipment further reduces operational costs.
- Providing rapid deployment capabilities compared to traditional inspection methods, significantly reducing downtime and improving response time.
- Optimizing monitoring procedures through various sensors and detectors, facilitating real-time data collection and analysis to: (i) identify threats, (ii) provide real-time situational awareness, (iii) ensure continuity of essential services, (iv) reducing disruptions and (v) limit playing a pivotal role in decision-making and mitigating risks.

The main arguments put forward by the partners, irrespective of their technical specifications, included:

- The ability to enhance and automate operations and enrich user experience from the utilization of AI technology;
- The reduced costs from the adoption of such technologies, which is a significant factor for market players in the industry due to the budget cuts they have to address;
- Safety and security, including passenger and personnel protection and welfare;
- Operational efficiency and performance and minimization of human errors.

The partners' contributions are included in a Table in Annex 2 regarding the technology each is contributing. To protect the partners' IPR and sensitive information, these Annexes will not be made publicly available.

A description of the exploitable technologies to which a partner contributes is included in Annex 3. To protect the partner's IPR and sensitive information, these Annexes will not be made publicly available.

4.3. Policy Plans & Regulatory Framework

For the purposes of the TESTUDO project, it is necessary to address the applicable legal and regulatory framework that may impact the technology innovations developed. The following legal frameworks have been identified (non-exhaustive) to govern the use and deployment of the technologies intended for the project.

4.3.1. Unmanned Aircraft Vehicles (UAVs)

EU Regulations 2019/945 of 12 March 2019 on unmanned aircraft systems and third country operations of unmanned aircraft systems and 2019/947 of 24 May 2019 on the rules and procedures for the operation

of unmanned aircraft (Regulations) set the framework for the safe operation of drones in European skies (EU and EASA Member States).

The Regulations are enforceable in all EU Member States as of 31 December 2020 and all unmanned aircraft systems manufacturers and operators must ensure they comply with their provisions. The Regulations do not distinguish between leisure or commercial activities for operations or UASs; a risk-based approach is followed considering the weight and other specifications of the UAS and the type of operation it is intended to complete.

4.3.2. GDPR

The General Data Protection Regulation GDPR (Regulation (EU) 2016/679) on a European level and the adoption of the GDPR on a national level and/or any additional local directives or guidelines issued to that extent is applicable to the TESTUDO activities and solutions.

The GDPR was formally adopted by the European Parliament in May 2016 and replaced the 1995 General Data Protection Directive (Directive 95/46/EC), which applies to all 28 EU member states and is effective from May 2018. Entities are subject to the GDPR as far as they process personal data of EU data subjects for their goods or service offerings in the EU and/or for the monitoring of the behaviour of EU data subjects taking place within the EU.

The GDPR has introduced new requirements and more stringent data protection challenges, backed by extremely high fines for non-compliance. GDPR is not just a compliance exercise but has major strategic implications that could bring market opportunities and competitive advantage for those who plan appropriately or potential revenue loss for those who fail to react.

Companies developing and deploying surveillance technologies must comply with GDPR to ensure the lawful and transparent use of data collected by their systems.

4.3.3. AI act by European Commission

The AI Act aims to provide AI developers, deployers and users with clear requirements and obligations regarding specific AI uses. The second iteration of this deliverable will address this in more detail.

4.3.4. Other relevant legislations and standards

- Surveillance and Monitoring Laws, and International Regulations and Cross-Border Data Transfers.
- Product Safety Directives: Directives such as the Machinery Directive (2006/42/EC) and the Electromagnetic Compatibility Directive (2014/30/EU) apply to aspects of chemical detector design and manufacturing due to communication, data transmission ensuring that they meet safety and performance standards.
- Environmental Directives: Directives like the Waste Electrical and Electronic Equipment (WEEE) Directive (2012/19/EU) and the Restriction of Hazardous Substances (RoHS) Directive

(2011/65/EU) may govern the use of certain materials or components within chemical detectors to minimize environmental impact and ensure proper disposal.

- **Safety and Security Regulations:** Depending on the intended application of chemical detectors (e.g., industrial safety, environmental monitoring, defence), various regulations related to safety, security, and emergency response planning may apply, such as the Seveso III Directive (2012/18/EU) for hazardous substances or regulations pertaining to border security and defence equipment or maritime regulations.
- **Product Safety Directives:** Directives such as the Machinery Directive (2006/42/EC) and the Electromagnetic Compatibility Directive (2014/30/EU) may apply to aspects of chemical detector design and manufacturing, ensuring that they meet safety and performance standards.
- **RoHS Directive (2011/65/EU):** The Restriction of Hazardous Substances Directive restricts the use of certain hazardous substances, including lead, mercury, cadmium, and others, in electrical and electronic equipment to reduce their environmental impact and promote recycling.
- **Environmental Directives:** Directives like the Waste Electrical and Electronic Equipment (WEEE) Directive (2012/19/EU) and the Restriction of Hazardous Substances (RoHS) Directive (2011/65/EU) may govern the use of certain materials or components within chemical detectors to minimize environmental impact and ensure proper disposal.
- **Regulation (EU) 2018/1139,** established on July 4, 2018, focuses on common rules in civil aviation within the European Union. This regulation aims to ensure a high and consistent level of safety in civil aviation by implementing shared safety standards. It amends various existing regulations and directives related to civil aviation, such as Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014, and Directives 2014/30/EU and 2014/53/EU of the European Parliament and Council. (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1139>).
- **Repealing Regulations (EC) No 552/2004 and (EC) No 216/2008** to streamline regulations in the field of civil aviation.
- **JARUS SORA,** which stands for Specific Operations Risk Assessment, is a methodology developed by the Joint Authorities for Rulemaking on Unmanned Systems (JARUS). This methodology is key in assessing the risks associated with specific unmanned aircraft system (UAS) operations. Determining the safety levels required for different UAS operations within the European Union is crucial.
- **Safety Standards:** Small mobile robots are typically subject to safety standards to ensure their safe operation and interaction with humans and the environment. These standards may cover electrical safety, mechanical safety, emissions, and risk assessment.
- **Radio Frequency Regulations:** If the mobile robot uses wireless communication technologies such as Wi-Fi or Bluetooth, it may need to comply with radio frequency emissions regulations and spectrum usage regulations.

- **Traffic and Transportation Regulations:** If the mobile robot operates in public spaces or interacts with vehicles or pedestrians, it may need to comply with traffic and transportation regulations.
- **Product Certification:** Depending on the jurisdiction and the specific market, small mobile robots may need to undergo product certification or testing to demonstrate compliance with relevant regulations and standards. This could include obtaining certifications such as CE marking in the European Union or FCC certification in the United States.

4.4. Technology Trends

For the Market Analysis, it is essential to identify the current technology trends. This information will be crucial for the consortium to use as a predictive indicator of the success of their innovations under TESTUDO in the relevant market sector. Current trends provide a valuable baseline for the entities to make informed decisions around long-term strategies for promoting and exploiting the technologies going forward.

Information on market trends can also help identify potential signals of industry shifts, presenting partners with tremendous opportunities to manoeuvre and align with the trends rather than oppose them.

Annex 4 presents a list of the current technology trends relevant to the innovations being developed in TESTUDO based on the information collected by the partners. Read and examined together with the Competitive Analysis, it enables us to locate business rivalry and assess partners' strengths so that partners can make the relevant adjustments and offer a competitive advantage over other existing and/or similar technologies.

For each of their assets the partners were requested to provide information as to:

- Why is there a move towards utilisation of their technology.
- Which industries would benefit the most from the use of their technology.
- What is the current market growth for their technology.
- What are the current uses and what could be the future uses of their technology.
- Whether steps have been taken towards utilizing/developing/regulating the technology.

4.5. Competitive Landscape

Input was gathered from partners to identify competitors of TESTUDO solutions and technologies and to draw the competitive landscape. Specifically, partners identified potential competitors to TESTUDO technologies and other competing solutions.

The first question on competition intensity aims to create a general image of the industry's competition. It is based on Michael Porter's "Five Forces" strategy tool (Porter, 1979).

Competitive Rivalry - How many rivals do you have? Who are they, and how does the quality of their products and services compare with yours?

Supplier Power - How many potential suppliers do you have? How unique is the product or service they provide, and how expensive would switching from one supplier to another be?

Buyer Power - How many buyers are there, and how big are their orders? How much would it cost them to switch from your products and services to rival ones? Are your buyers strong enough to dictate terms to you?

Threat of Substitution—An easy and cheap substitution can weaken your position and threaten your profitability.

Threat of New Entry -How easy is getting a foothold in your industry or market? How much would it cost, and how tightly is your sector regulated? In essence, partners provided input based on an indicative set of questions, listed below, to accurately identify the competition landscape relevant to their innovation.

The input provided by the partners is presented in Annex 4.

4.5.1. Market Analysis Survey

A survey, a copy of which is attached in Annex 5, was shared with the consortium partners to gather information regarding the partners' potential customers and assess the current market opportunities and market size. Based on the input received by the partners, an initial analysis of the potential customers, market size and competition is provided below.

Target Customers

Through the «Market Analysis» questionnaire, consortium partners answered questions regarding the target group of their exploitable technologies or the technologies to which they contributed.

Figure 1 demonstrates the most common target customers for the exploitable technologies of the TESTUDO project. The leading category is «End users» with sixteen responses, confirming that the primary target customers for the TESTUDO solution in the future may be End users.

The second most predominant categories are Small and medium Enterprises (SMEs) and National Governments, receiving nine answers. These categories are followed by «Industry security market operators» and «Technical innovators». The chart also includes the category «Other» where partners mentioned target groups such as «First responders, architecture, engineering, construction, media and entertainment, automotive and transportation, logistics, aerospace and defence».

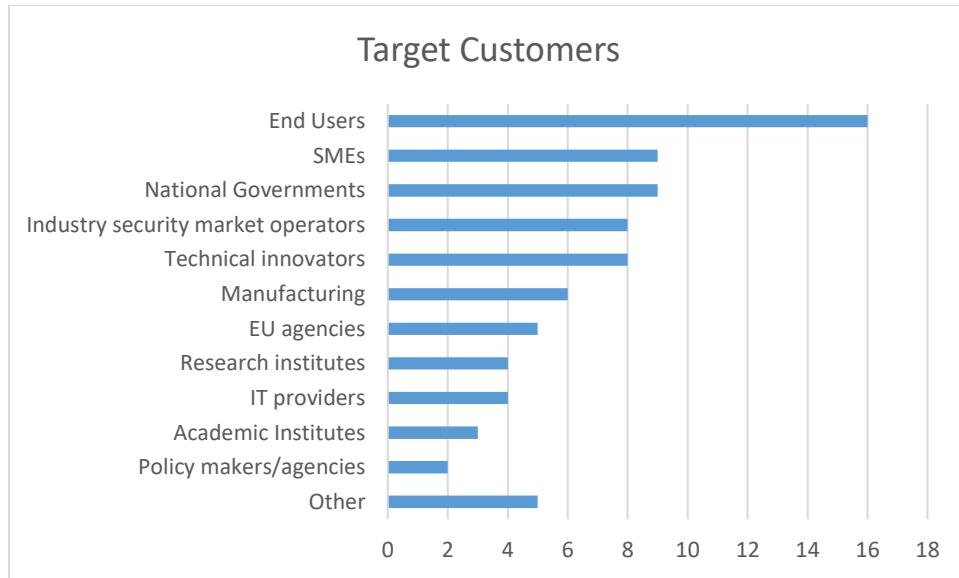


Figure 1. Target Customer.

Broader customer or adopter

Figure 2 illustrates the types of broader customers identified by partners. The most common broader customer category, with sixteen answers, is «Customer who would potentially pay». Following this, the categories «Adopter of our use case» and «Trial adopter» received the highest responses. Lastly, one partner answered «Other», which includes broader customers such as «Technology partners with supplementary IPR».

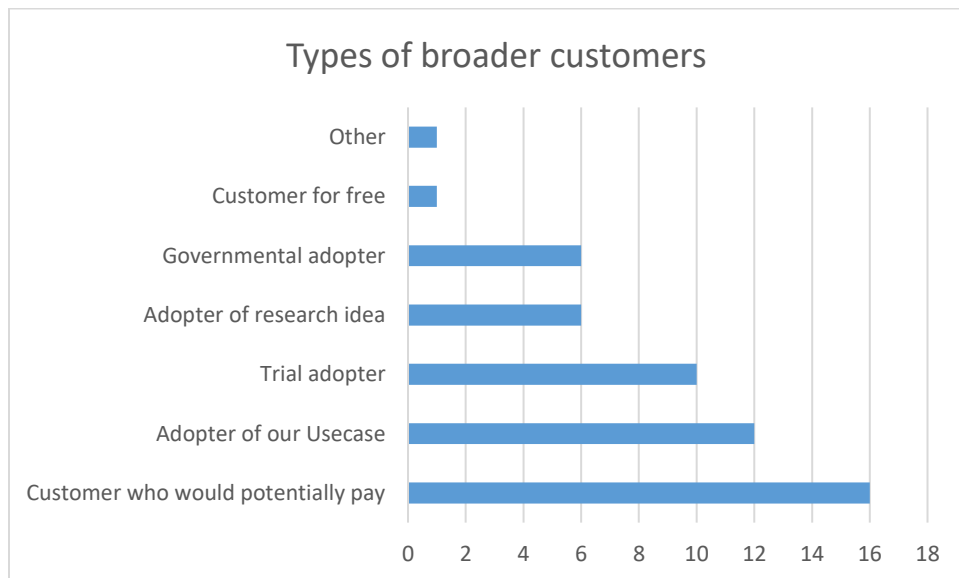


Figure 2. Broader customers.

Market

Through the «Market Analysis» survey, partners were asked to describe the markets where their exploitable assets operate. The results presented in Figure 3 indicate that all the exploitable assets are in emerging markets, except for one in a market-creating phase and another that is both emerging and market-creating simultaneously. Based on these findings, the TESTUDO solution is expected to enter emerging markets.

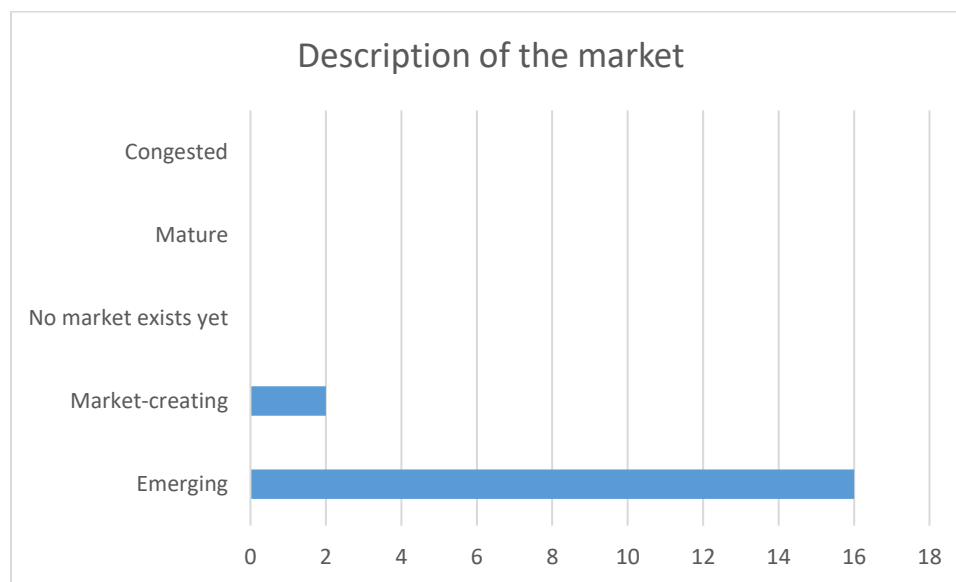


Figure 3. Description of the market.

Market size

Regarding the existing markets, partners gave information about their size of the market that their exploitable asset take part. As presented in Figure 4, the majority are in market that have some presence, two in isolated niche markets, and one in a common market size.

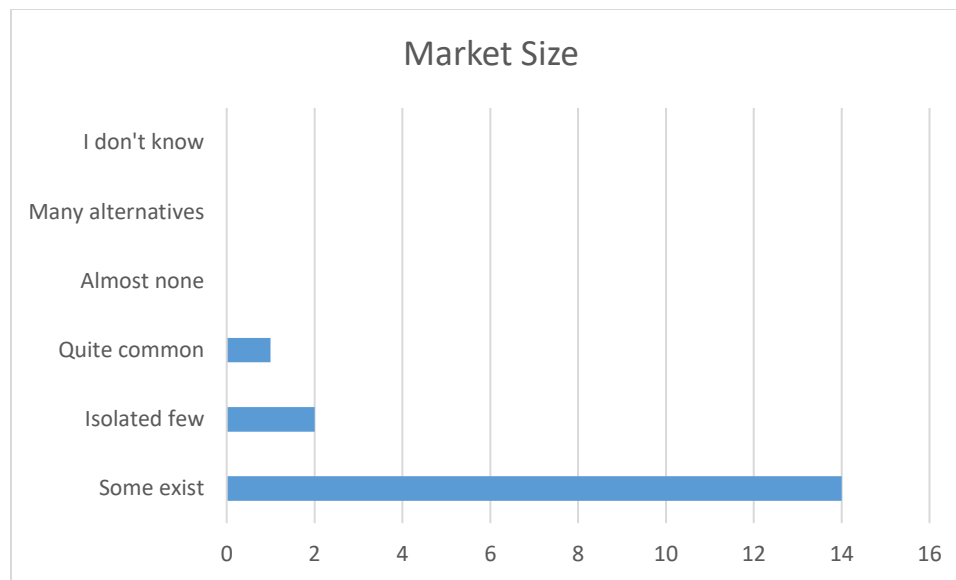


Figure 4. Market size.

Alternatives/Competition

The last part of the survey focuses on alternative choices and the competition that exploitable assets face. Based on responses from partners, a picture of the competitors in the market relative to TESTUDO's exploitation assets has been developed. The most common response was «Comparable research initiatives» with thirteen answers. This is followed by «Potential collaborators,» with ten responses. «Direct Competitors» and «Substitutes with no same solution» are the least common choices among partners. The partner's input is reflected in Figure 5.

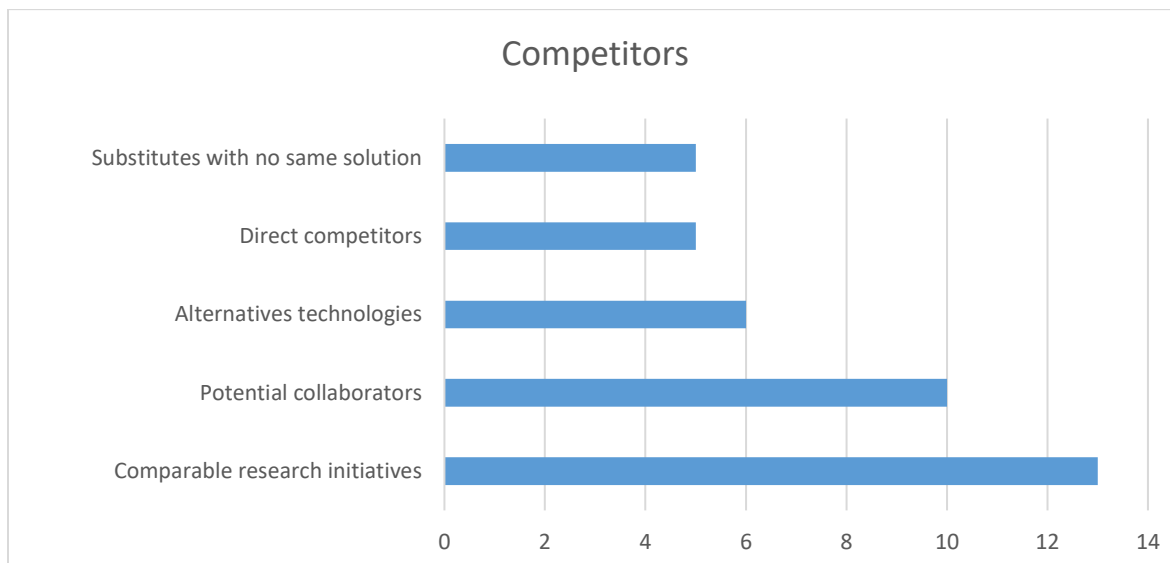


Figure 5. Competitors.

Figure 6 presents the current competitors and how common they are. The majority of the exploitable assets face some competition. Three assets have little competition, while three have quite common. One asset has almost none.

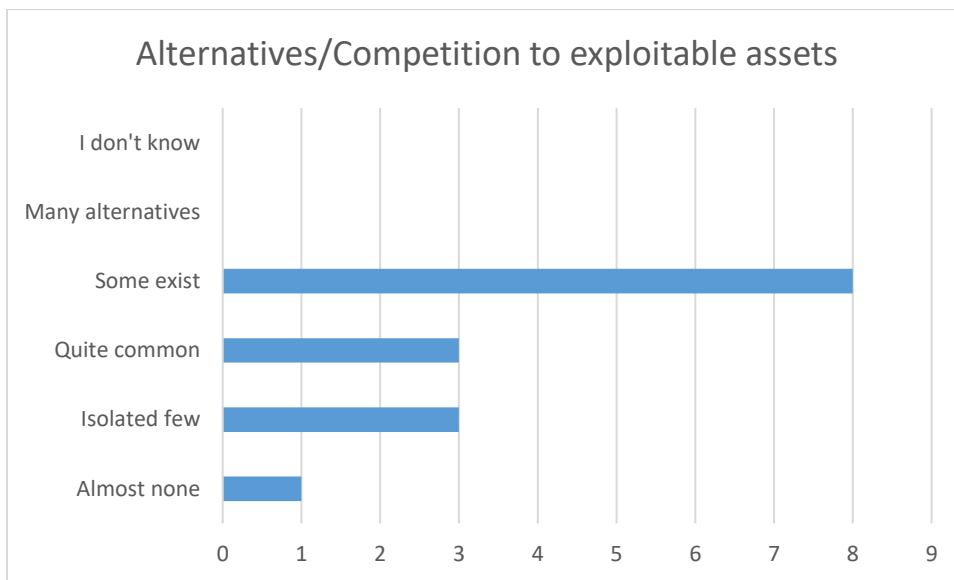


Figure 6. Alternatives/Competition to exploitable assets.

Figure 7 describes how mature the competition is in the market where the exploitable assets are established. Almost all partners answered that the competition is average. Only three exploitable assets face a different level. One exploitable asset's maturity is very strong, one is somewhat weak, and one is weak. This concludes that the TESTUDO solution will probably have an average competitive maturity.

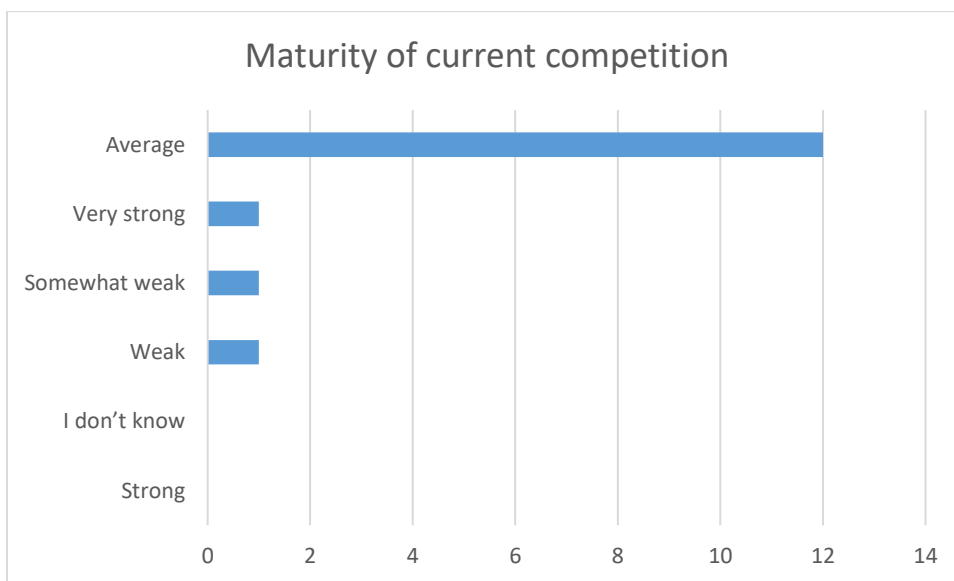


Figure 7. Maturity of current competition.

5. Socioeconomic Analysis

5.1. Project PESTLE Analysis

This PESTLE analysis examines the Political, Economic, Social, Technological, Legal, and Environmental factors affecting the project, identifying opportunities and risks that may impact its execution and long-term sustainability.

Political Factors

The EU's security policies and funding programs strongly support initiatives like TESTUDO, particularly cybersecurity, AI regulation, and infrastructure protection. The European Commission (EC) has prioritized critical infrastructure resilience, and TESTUDO aligns well with these objectives by offering autonomous, AI-driven security solutions.

However, several political risks could impact the project. Regulatory changes such as the upcoming AI Act and updates to GDPR may impose new restrictions on AI-powered surveillance systems, requiring continuous compliance updates. Geopolitical tensions and significantly rising cybersecurity threats from state-sponsored attacks may shift EU priorities towards cyber warfare defence, potentially diverting funding from infrastructure protection initiatives like TESTUDO.

Changes in political leadership within EU member states could lead to altered funding priorities, affecting project financing and market adoption. Additionally, additional bureaucratic and security clearance requirements could arise if TESTUDO is considered strategically significant for defence applications, complicating international collaborations.

Despite these risks, the EU remains highly invested in technological innovation for security. If TESTUDO can demonstrate alignment with EU security frameworks and compliance with regulations, it will receive strong political and institutional support.

Economic Factors

The TESTUDO project benefits from a strong European investment climate in security, AI, and robotics. The market for autonomous security solutions is rapidly expanding, driven by demand from governments, private infrastructure operators, and security firms.

Key economic opportunities include stable EU funding through Horizon Europe, ensuring financial security during development. The global market for AI-driven security systems is growing, creating commercialization opportunities for TESTUDO's technologies. By reducing human involvement in security operations, TESTUDO offers long-term cost savings for governments and private companies responsible for critical infrastructure protection.

Economic risks include high development costs due to the complexity of AI, UAVs, and cybersecurity solutions, which require substantial R&D investment. Many public infrastructure operators may lack the budget to adopt high-tech autonomous security systems, requiring alternative business models such as leasing or service-based offerings. Economic recessions or financial crises in the EU could lead to the

reallocation of security funding to immediate economic recovery measures, reducing available financing for projects like TESTUDO.

The project's reliance on government contracts could pose challenges if political priorities shift away from infrastructure security investments. TESTUDO should diversify funding sources to mitigate economic risks, explore public-private partnerships, and develop scalable, cost-effective deployment models to make adoption more attractive.

Social Factors

Public perception and societal acceptance of AI-driven security solutions will be crucial in TESTUDO's adoption and success.

Growing awareness of security threats, including cyberattacks and terrorist threats, has increased public demand for enhanced security measures. AI-powered surveillance and threat detection are becoming more mainstream, leading to greater public trust in autonomous security solutions. Additionally, TESTUDO reduces the need for human security personnel in hazardous environments, improving workplace safety for first responders and security teams.

However, privacy concerns remain a significant challenge. AI-powered surveillance, especially using UAVs, facial recognition, and automated monitoring, raises concerns about data privacy and civil liberties, potentially leading to public opposition or regulatory backlash. Ethical considerations regarding AI decision-making in security applications could also impact public acceptance, particularly if AI-driven threat assessment systems lead to wrongful identifications or errors.

To address these concerns, TESTUDO must ensure compliance with GDPR, implement ethical AI frameworks, and communicate transparently with stakeholders to build public trust.

Technological Factors

TESTUDO operates at the cutting edge of AI, robotics, cybersecurity, and digital twins, giving it a competitive advantage. The project integrates autonomous UAVs/UGVs, AI-based threat detection, and secure network infrastructure for real-time monitoring and response.

The increasing adoption of AI, 5G networks, and edge computing enhances the potential of TESTUDO's autonomous security systems. AI-powered cybersecurity tools improve resilience against cyber threats, and digital twins enable real-time simulation and predictive analysis of security scenarios.

However, technological risks include interoperability challenges, cybersecurity vulnerabilities, and the rapid evolution of AI and robotics, which could make some of the project's solutions obsolete before commercialization. Integration challenges with existing security infrastructure could slow adoption by public and private sector clients. Additionally, compliance with AI regulations, such as the EU's AI Act, may require continuous updates to ensure adherence to ethical AI principles and safety standards.

TESTUDO should focus on modular and adaptable system architectures to mitigate technological risks, ensure seamless integration with existing infrastructure, and be flexible for future technological advancements.

Legal Factors

The project must comply with EU regulations on AI, data privacy (GDPR), and drone operations (EASA regulations for UAVs). The European AI Act is expected to impose stricter guidelines on AI applications, particularly in surveillance and security domains.

Legal risks include potential restrictions on AI-powered surveillance under data protection laws, requiring precise data collection, storage, and usage policies. Cross-border data-sharing restrictions could impact multinational security operations' real-time threat detection and response capabilities.

IPR management will be crucial for commercializing TESTUDO's technologies. Ensuring clear ownership structures for AI algorithms, cybersecurity solutions, and UAV/UGV software will be necessary to avoid legal disputes among project partners.

To address these legal challenges, TESTUDO engages legal experts to ensure full compliance with evolving EU regulations, establish clear IPR agreements among consortium members, and implement robust data protection policies.

Environmental Factors

TESTUDO aligns with sustainability goals by reducing reliance on human-operated surveillance, often involving fuel-powered patrol vehicles, extensive travel, and energy-intensive monitoring infrastructure. By deploying autonomous UAVs and UGVs with energy-efficient technologies, TESTUDO helps lower emissions, minimize resource consumption, and reduce the overall carbon footprint of security operations.

However, the environmental impact of UAV and UGV manufacturing, battery usage, and electronic waste must be addressed. The increasing deployment of autonomous systems in security operations raises concerns about sustainability, requiring responsible disposal and recycling strategies.

Climate change-induced extreme weather events, such as wildfires and floods, could also create operational challenges for UAVs and surveillance systems. TESTUDO must ensure its technology is resilient to harsh environmental conditions to maintain reliability in real-world security applications.

TESTUDO can enhance its environmental sustainability while aligning with the EU's green transition goals by integrating sustainable energy solutions, such as solar-powered UAVs or energy-efficient computing.

5.2. Project SWOT Analysis

A SWOT analysis is a technique for strategic planning that evaluates the Strengths, Weaknesses, Opportunities, and Threats related to a project or a business venture. It requires defining the goal of the project or venture and identifying the internal and external factors that can help or hinder its achievement. A regular examination of the environment in which an organization operates helps anticipate the changing trends and incorporates them into the organization's decision-making process.

Because of the dynamic and increasingly competitive environments in which institutions operate, it is vital, for both the Project and the future planning of each partner for exploitation and commercialization of the technologies, to assess the extent to which such environments will influence them. SWOT analysis

is a step that helps organizations to analyse their competitiveness and identify factors that can either stimulate or threaten their objectives.

Therefore, before presenting TESTUDO's business potential, a SWOT analysis must be performed to identify the basics of its Strengths, Weaknesses, Opportunities, and Threats.

Partners were given the following SWOT Table template to assist their analysis and responses:

	Partner Name and Technology title	
	Favourable factors	Adverse factors
Internal factors	STRENGTHS What do you do well? What unique resources can you draw on? What do others see as your strengths?	WEAKNESSES What could you improve? Where do you have fewer resources than others? What are others likely to see as a weakness?
External factors	OPPORTUNITIES What opportunities are open to you? What trends could you take advantage of? How can you turn your strengths into opportunities?	THREATS What threats could harm you? What is your competition doing? What threats do your weaknesses expose you to?

Table 3. SWOT Analysis Template.

According to the SWOT analysis provided by the partners for their respective asset, TESTUDO technologies possess several key strengths. These include advanced AI methods, a holistic overview, and potential statuses for the CI virtual replicas under the simulated events. Additionally, AI techniques can automate the detection process, increasing the accuracy of the required detections and optimizing the use of operational resources. Also, aerial and ground vehicles with sensors enhance the collection of data in inaccessible and dangerous areas. On the other hand, TESTUDO faces some weaknesses or challenges that need attention and will be examined further with the final TESTUDO platform.

In the broader context, TESTUDO has various opportunities, such as the potential extension of services to other types of security and different environments. TESTUDO nevertheless faces some threats, including various legislative barriers from each partner's differing authorities and legal issues that may delay the project's progress.

	Overall SWOT analysis	
	Favourable factors	Adverse factors
Internal factors	STRENGTHS <ul style="list-style-type: none"> Real operational picture (data) in large area with low connectivity territory. Enhanced security monitoring capabilities and threats response times in water facilities. 	WEAKNESSES <ul style="list-style-type: none"> Some exploitable assets have low technological maturity and face challenges related to staffing, training, operation, and maintenance costs, primarily due to the high skillset requirements for staff.

	<ul style="list-style-type: none"> • Exploitable assets can host multiple payloads (thermal RGB, multispectral, Lidar cameras). Also, they do precision automated actions. Some action become straightforward by using these exploitable assets. • Using unmanned vehicles, the duration of the pilot may last up to one hour giving the opportunity of more flexibility. • These exploitable assets offer a real-time analysis of network traffic, no required labelled data for training are needed allowing having an automated training. • The advanced AI methods offer detailed accurate data. Using these sensors, it is enhanced surveillance capabilities. • Additionally, the sensors can sense purely passive and capture the scene's appearance and present objects. • New methods based on AI techniques will be able to automate the detection process, increase the accuracy of the required detections, and optimize operational resources. • An adaptability to different Cis and scenarios needs is provided. • Exploitable assets have low power consumption increasing the continuous use time of them. • High mobility, easy to deploy, light and small assets are used in TESTUDO project. • Reduced time and effort required for maintenance. • High degree of scalability to handle large numbers of resources and tasks. Lastly, modularity, scalability and flexibility are features of the exploitable assets. 	<ul style="list-style-type: none"> • Additionally, relatively high memory consumption is another significant weakness. Integrating AI components into exploitable assets is complex, and the accuracy and reliability of the captured data can sometimes be challenging to ensure. Implementing advanced predictive analysis techniques may require precise detection outcomes and data streams, often limited in availability. • The effectiveness of model training also depends heavily on the quality and quantity of data. • Furthermore, the fragility of exploitable assets may hinder their functionality, while limited operational time and the lack of autonomous docking capabilities can negatively affect their usability. • Finally, consolidating sensitive security data into a single platform raises concerns about data security and privacy, necessitating robust access controls, encryption, and strict compliance with data protection regulations.
External factors	<p style="text-align: center;">OPPORTUNITIES</p> <ul style="list-style-type: none"> • The mass production of exploitable assets reduces costs, enabling scalability to new potential infrastructures. This also enhances 	<p style="text-align: center;">THREATS</p> <ul style="list-style-type: none"> • The concept of some exploitable assets may be copied by organisations with greater financial and technological leverage.

	<p>the capability to commercialize deep tech and expand the product portfolio.</p> <ul style="list-style-type: none"> • Additionally, improving and testing the prediction model's accuracy on benchmark datasets presents another significant opportunity. • The reduction in memory consumption opens new possibilities. At the same time, the increasing demand for advanced mapping solutions for critical infrastructure security and monitoring, combined with advancements in AI and computer vision, improves the accuracy and speed of 3D mapping and facilitates expansion into new markets. • Several exploitable assets have the potential to be applied across various sectors beyond surveillance and construction. • Moreover, advancements in AI and machine learning create opportunities for continuous improvement and enhancement of the asset's performance in accuracy, relevance, and responsiveness. • Collaborating with industry partners, users, and other research institutions within the project scope fosters the exchange of knowledge and resources, driving innovation and market penetration. • This approach can address the growing demand for advanced CI security and surveillance technologies. • Opportunities for collaboration in manufacturing among consortium partners present significant potential. • There is also growing demand in sectors such as environmental monitoring, industrial safety, and defence, offering new avenues for growth and application. 	<ul style="list-style-type: none"> • Additionally, local legislative barriers and a lack of regulation pose significant challenges for the partners. • Emerging competition in the industry presents a threat to the success and viability of the exploitable assets too. Rapid advancements in AI, sensor technology, and mapping solutions may render these exploitable assets obsolete or less competitive. Increased surveillance capabilities may raise concerns regarding privacy and regulatory compliance. • Unexpected events, system failures, or inaccuracies in predictive analytics outputs could undermine operators' confidence in the reliability of the assets. • Cybersecurity issues also pose a significant threat, as they can compromise the integrity, confidentiality, or availability of resources and sensitive information.
--	--	--

Table 4. SWOT Analysis.

6. Stakeholder Identification and Analysis

Effective stakeholder identification and analysis is essential for successfully implementing innovative security solutions and their long-term impact. TESTUDO is a large-scale European initiative combining cutting-edge autonomous systems, AI-driven surveillance, UAVs, UGVs, cybersecurity measures, and digital twins to strengthen CI protection. Given its interdisciplinary nature and diverse applications, the project engages a broad ecosystem of stakeholders across public, private, and regulatory sectors. Understanding these stakeholders is key to ensuring regulatory compliance, market adoption, and sustainable deployment of TESTUDO's technologies.

6.1. Types of Stakeholders Characterization

TESTUDO's stakeholder ecosystem includes governmental, industrial, academic, and societal actors. These stakeholders can be grouped into the following categories:

Public Sector and Regulatory Authorities

This group comprises government agencies, regulatory bodies, and policymakers responsible for overseeing AI-driven security solutions' security, technology, and ethical compliance.

- EU Institutions and Funding Agencies: The European Commission, Horizon Europe, and related funding bodies that drive research, innovation, and regulatory frameworks.
- National and Local Governments: Ministries of Defence, Interior, and Public Security that implement national security policies.
- Regulatory Agencies: EASA, GDPR enforcement bodies, and AI ethics committees overseeing drone and AI regulations.
- Law Enforcement and Emergency Services: Police forces, fire brigades, and disaster response units will use TESTUDO's technologies for real-time threat monitoring.

Industry and Private Sector Stakeholders

TESTUDO's commercialization and market deployment depend on industry partners that develop, integrate, or adopt the technology.

- Critical Infrastructure Operators: Organizations managing transport, energy, water, and communication networks, which require advanced security and surveillance solutions.
- Security and Defence Contractors: Private firms specializing in surveillance, cybersecurity, and AI-based security solutions, which may integrate TESTUDO technologies into their services.
- Technology Providers: Companies in AI, robotics, IoT, and cybersecurity that develop or integrate components such as UAVs, UGVs, sensor systems, and AI algorithms.
- End-User Organizations: Large-scale corporate security firms, facility management companies, and smart city developers that might implement TESTUDO for urban security solutions.

Research and Academic Institutions

TESTUDO is driven by scientific advancements in AI, cybersecurity, and autonomous systems, making research institutions key players.

- Universities and Research Centres: Institutions researching machine learning, AI ethics, UAV/UGV navigation, and cybersecurity.
- EU-funded R&D Networks: Research collaborations in Horizon Europe and similar EU programs, ensuring knowledge exchange and technology transfer.
- Cybersecurity and AI Ethics Think Tanks: Organizations focusing on the ethical, social, and legal implications of autonomous surveillance and AI-driven threat detection.

Civil Society, Ethics, and Policy Advocacy Groups

The deployment of AI-driven security raises ethical, legal, and privacy concerns. Several stakeholder groups advocate for responsible AI deployment and regulatory compliance.

- Privacy and Digital Rights Organizations: Groups like EDRi (European Digital Rights) that focus on GDPR compliance, surveillance ethics, and AI governance.
- Human Rights and Ethics Watchdogs: NGOs monitoring the impact of AI-driven security technologies on civil liberties.
- Public Interest and Community Groups: Local communities concerned about privacy, public safety, and the use of AI in surveillance.

End-Users and Workforce Stakeholders

TESTUDO's successful adoption depends on how end-users, security professionals, and infrastructure operators interact with its solutions.

- Security Personnel and First Responders: Police, firefighters, and paramedics who will use the system for rapid response and decision-making.
- Drone and Robotics Operators: Professionals responsible for managing UAV/UGV fleets for security monitoring.
- Public Sector IT and Security Managers: Experts handling network security, data privacy, and AI system management.

Each group has different levels of influence, expectations, and concerns, which are analyzed in the next section.

6.2. Stakeholders Analysis

Public Sector and Regulatory Authorities

The European Commission and Horizon Europe funding bodies provide financial support and regulatory frameworks, ensuring compliance with EU security and AI policies. They are highly influential in determining the success and scalability of TESTUDO's technologies. Regulatory agencies like EASA and

GDPR enforcement bodies shape the legal landscape by defining drone flight regulations, data privacy protections, and AI compliance requirements.

Challenges and Considerations:

- **Regulatory Uncertainty:** New laws, such as the AI Act and updates to GDPR, may introduce compliance hurdles.
- **Data Privacy Concerns:** Regulations around biometric surveillance, AI-driven facial recognition, and cross-border data sharing need careful adherence.
- **Drone and Airspace Regulations:** Ensuring compliance with EU drone laws for critical infrastructure security applications.

Strategic Engagement:

- **Proactive Policy Alignment:** Collaborate with EU policymakers to ensure regulatory alignment and secure long-term funding.
- **Ethical AI and Compliance Frameworks:** Establish GDPR-compliant AI governance models to address privacy concerns.
- **Joint R&D with Security Agencies:** Engage with law enforcement and emergency services to optimize real-world deployment scenarios.

Industry and Private Sector Stakeholders

Security, AI, and robotics companies will be primary TESTUDO adopters and commercial partners. Critical infrastructure operators (power grids, water utilities, transport hubs) most need TESTUDO's threat monitoring capabilities.

Challenges and Considerations:

- **Cost of Implementation:** High initial investment costs could slow adoption.
- **Interoperability with Legacy Systems:** Integrating TESTUDO with existing CI security frameworks could require customized deployment strategies.
- **Market Competition:** Competing AI-based security surveillance systems from major defence and security firms pose a challenge.

Strategic Engagement:

- **Custom Business Models:** Offer flexible financing (leasing, as-a-service models) to encourage adoption.
- **Technology Standardization:** Develop plug-and-play solutions that seamlessly integrate into existing security architectures.
- **Industry Partnerships:** To accelerate market entry, form alliances with defence contractors, security firms, and AI technology providers.

Research and Academic Institutions

Universities and R&D centres are key in innovation, pilot testing, and ethical AI development. Their contributions to TRL (Technology Readiness Level) progression, AI safety, and machine learning validation will enhance TESTUDO's credibility.

Challenges and Considerations:

- Academic-industry gap: Bridging the divide between academic research and real-world application.
- Publication vs. Proprietary IP: Balancing open science principles with intellectual property protection.

Strategic Engagement:

- Joint Research Collaborations: Co-develop AI security standards with leading universities.
- Ethical AI Frameworks: Publish research on bias mitigation, AI transparency, and human-in-the-loop models.

Civil Society and Ethics Watchdogs

Public trust is critical for TESTUDO's adoption. Privacy advocacy groups may challenge AI-powered surveillance, citing mass surveillance concerns and potential abuse.

Challenges and Considerations:

- Surveillance Ethics: Addressing concerns over privacy violations and AI bias.
- Public Perception Risks: Fear of job displacement in security professions.

Strategic Engagement:

- Transparent AI Policies: Ensure ethical AI use and avoid misuse in mass surveillance.
- Public Awareness Campaigns: Engage citizens on AI safety and GDPR compliance.

7. Individual Exploitation Plans

This section presents the Individual Exploitation Plans for project partners involved in developing ERs. Each partner's plan outlines how they will utilize, commercialize, or further develop their respective ERs beyond the project's completion. This includes market potential, commercialization strategies, licensing models, intellectual property considerations, and research pathways.

SINTEF

SINTEF is responsible for the Maximized Surveillance Swarm Intelligence Module and the Autonomous Resource Allocator Module. These modules optimize the deployment of UAVs and UGVs for real-time surveillance, improving coverage and efficiency in CI security. As a non-profit research institute, SINTEF plans to integrate these modules into future research and collaborate with industry partners to refine the technology. The modules will be used in public security, defence, search and rescue, and industrial monitoring. SINTEF does not intend to commercialize the technology directly but may license it to industrial stakeholders or explore spin-off companies as it matures. The estimated time to market is four years, requiring further hardware validation and interoperability improvements.

CEA

CEA has developed the Network Infrastructure module, which manages wireless multi-hop communications for secure UAV/UGV operations, and the Cyber-Threat Detection Module, an anomaly-based intrusion detection system. CEA's primary strategy is knowledge expansion and further R&D collaboration with industry partners. The Cyber-Threat Detection Module has strong potential in network security and critical infrastructure protection. The Network Infrastructure module will be further developed for real-time security monitoring in complex environments. CEA does not plan for immediate commercialization but will integrate its results into cybersecurity research and explore industry licensing. Depending on further validation and integration with cybersecurity standards, the estimated time to market is four years.

CERTH

CERTH has developed multiple exploitable results, including the Visual Detection Module, the Multispectral Detection Module, the Prediction and Simulation Models, and the Optimized 3D Mapping Module. These technologies enhance AI-based object detection, surveillance automation, and predictive security analysis. CERTH will use these modules to advance AI-driven security solutions and to improve its research capabilities. The Visual Detection and Multispectral Modules will be refined for law enforcement, emergency response, and private security applications. The 3D Mapping Module will be applied in urban planning, security, and infrastructure monitoring.

The estimated time to market varies: the Visual Detection and Multispectral Modules are expected within two to three years, while the Prediction and Simulation Models require further dataset validation before commercialization.

TEKNIKER

TEKNIKER has developed the Detection Module on Embedded Platforms and Low-Power Hardware Architectures for Machine Vision Applications at the Edge. These modules enhance AI-driven detection in embedded systems, enabling autonomous surveillance and real-time threat analysis. TEKNIKER plans to integrate these results into its real-time AI vision processing research. Strong commercialization potential exists for defence, environmental monitoring, and security applications. TEKNIKER may pursue licensing agreements with security technology firms and develop further customized AI-driven security solutions. The estimated time to market is four years, with further optimization of AI processing models required to improve accuracy and efficiency.

T4i

T4i has developed the CBRN Detection Tools, which enhance real-time airborne chemical detection for hazardous environments. This module has strong commercial potential due to the growing demand for CBRN monitoring solutions in the industrial, emergency response, and defence sectors. T4i will integrate this technology into its existing DOVER system and begin commercial deployment within three months of project completion. The technology will be marketed to tunnel operators, law enforcement, fire brigades, and environmental agencies. The commercialization strategy includes partnerships with drone manufacturers and security service providers to accelerate adoption.

VICOM

VICOM has developed the Visual Activity Recognition Module and the Traffic Anomaly Dataset. These technologies improve real-time surveillance, anomaly detection, and traffic monitoring. VICOM plans to license the Visual Activity Recognition Module to CCTV system integrators and smart city developers. The Traffic Anomaly Dataset will be publicly available to support AI-based traffic security research. The estimated time to market is three years, focusing on enhancing performance for real-world applications and expanding security analytics offerings.

ACCELI

ACCELI has developed the CERBERUS and DIOPTRA UAV prototypes, which have been designed for autonomous security monitoring and over-ground surveying. These UAVs are intended for public safety, critical infrastructure protection, and border security applications. ACCELI's strategy is commercialization through mass production and strategic partnerships. The company aims to refine prototypes, improve manufacturing efficiency, and expand market reach. The estimated time to market is two years, and the expected return on investment (ROI) is 20–30%. ACCELI may also develop new UAV product lines for environmental monitoring and disaster response.

DFKI

DFKI has developed the Site Scouting UGV, a high-mobility, all-terrain ground vehicle for disaster site exploration and autonomous monitoring. DFKI sees significant commercialization potential in disaster management, environmental monitoring, and security applications. The primary exploitation strategy is further research in publicly funded R&D projects plus commercialization through a spin-off company. The estimated time to market is three years, with plans to enhance system autonomy and improve navigation capabilities.

ENG

ENG has developed the Situation Awareness Framework for Enhancing CI Resilience (SAFER) and the Enriched Data Model for CI Protection. TESTUDO plays a major role in enforcing the Engineering market potential in the safety and security sector. TESTUDO is directly aligned with this strategy, bringing the long-standing R&D expertise of Engineering in information processing and situational awareness tools closer to the markets through pilots deployment of advanced solutions. Moreover, the TESTUDO results could also be a new step in the research on innovative technologies and solutions to be adopted in the emergency management domain, which will improve their offer to its Italian customers, including the Italian Ministry of Interior, the Italian Civil Protection and several LEAs, as well as in the context of European research projects and initiatives. Finally, it will be exploited the ENG stakeholders' list to ensure the public outreach of the project's activities as well as to enlarge the Pan-European Stakeholders Group.

CENTRIC

CENTRIC has developed XR Technologies Components, an extended reality (XR) application for security command and control (C2) operations. The exploitation strategy includes further R&D to refine XR applications and expand compatibility across different XR headsets. CENTRIC plans to integrate this result into future research projects, particularly in situational awareness and security training. Pilot implementations are expected within two years, with commercialization dependent on hardware advancements in the XR industry.

CENTRIC has developed a multimodal data fusion component. The exploitation strategy for this includes further R&D to integrate the component into a future larger system, adding data fusion capabilities to the module. This will become a key feature in future projects. The fusion module can also be exploited as a separate entity for projects that do not require a wholesale OSINT solution. The fusion component is expected to be fully operational by the end of the UC3 for TESTUDO.

8. Conclusions

The TESTUDO project has developed a comprehensive exploitation strategy and impact assessment framework to ensure its research outcomes are successfully transitioned into real-world applications. This deliverable evaluates the project's exploitable results, market positioning, stakeholder engagement, and intellectual property rights management. The findings of this document lay the groundwork for a more detailed market analysis and final impact assessment, which will be further elaborated in Deliverable D12.2.


One of the key takeaways from this analysis is the identification of multiple ERs, covering a range of innovative technologies, including AI-driven surveillance modules, cybersecurity solutions, multispectral detection systems, UAV and UGV platforms, and digital twins. The project has successfully categorized these ERs based on their TRLs and mapped out their commercialization potential. While some solutions are already nearing market readiness, others require further development and validation through real-world pilot deployments.

The Intellectual Property Rights strategy ensures that ownership and licensing agreements are clearly defined for all project innovations. This structured approach balances knowledge dissemination with proprietary protection, allowing TESTUDO partners to maximize the impact of their research outputs while fostering collaboration with industry and research institutions. Different protection mechanisms such as patents, copyrights, and open-access dissemination have been explored to tailor IPR management to the specific needs of each partner and technological result.

A preliminary market and competition analysis has provided insights into the business environment in which TESTUDO technologies will operate. The report highlights the growing demand for AI-powered security solutions, the increasing adoption of autonomous surveillance technologies, and the evolving regulatory landscape for UAVs and cybersecurity. The competitive analysis benchmarks TESTUDO's innovations against existing market players, ensuring its technologies remain competitive and aligned with industry standards.

The socioeconomic impact assessment, conducted using PESTLE and SWOT analyses, has identified opportunities and challenges that may affect the long-term adoption of TESTUDO's solutions. Political and regulatory factors, including EU AI and cybersecurity laws, will shape the project's deployment strategy. Economic considerations such as funding availability and market adoption barriers will influence commercialization timelines. Social and ethical concerns regarding AI-powered surveillance and data privacy must be addressed through robust compliance frameworks. Meanwhile, technological advancements, such as AI-driven threat prediction and real-time monitoring, present significant opportunities for expanding TESTUDO technologies across various industries.

A stakeholder identification and engagement strategy has been mapped out to ensure TESTUDO's successful adoption and sustainability. Key stakeholders include public sector regulatory bodies, industry leaders, research institutions, law enforcement agencies, and civil society groups. The engagement strategy focuses on regulatory compliance, industry partnerships, and public awareness initiatives to facilitate the adoption of TESTUDO's security solutions.



The individual exploitation plans for each project partner outline specific commercialization or research pathways. Some partners aim for direct market entry through licensing agreements and technology spin-offs, while others prioritize further R&D collaborations or integration into existing security frameworks. The expected time to market for most exploitable results varies between two and four years, with multiple partners exploring partnerships and funding mechanisms to accelerate adoption.

This deliverable sets the foundation for ensuring that TESTUDO's technologies transition beyond the research phase into operational security solutions for critical infrastructure protection. The insights provided in this report will inform the project's next phase, leading to a more refined market strategy, final impact assessment, and policy recommendations in Deliverable D12.2. By aligning technological innovations with market demands and regulatory frameworks, TESTUDO is well-positioned to contribute to the future of AI-driven security and resilience for critical infrastructure.

References

Anduril Industries. (n.d.). Command & Control. Retrieved March 4, 2025, from <https://www.anduril.com/command-and-control/>.

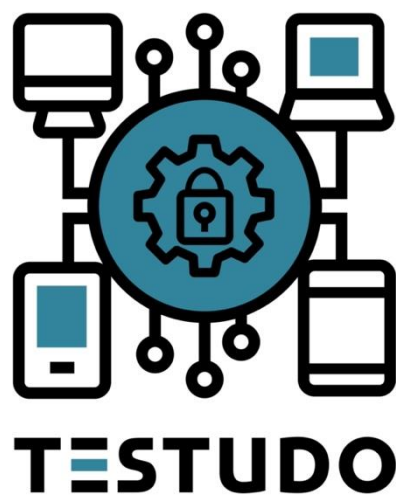
Darktrace. (2025). AI network security protection. Retrieved from <https://darktrace.com/products/network>.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Michael E. Porter, "[How Competitive Forces Shape Strategy](#)", *Harvard Business Review*, May 1979 (Vol. 57, No. 2), pp. 137–145.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Annex 1 – Template for Market Analysis Report - Partners Fill-In Form



TESTUDO

HORIZON-CL3-2022-INFRA-01- Grant Agreement No. 101121258

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES IN
INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

Market Analysis Report Partner Fill-in Form

This document serves as a guide for all partners participating in Task 11.3: Market analysis and potential business models in preparing Deliverable 11.3: Exploitation plans and impact pathways assessment.

All partners are required to fill-in all the relevant information below for the deliverable.

This deliverable provides a detailed market analysis, including the competitive landscape relevant to the technologies to be developed under the project and the proposed business models for promoting the technologies.

Please follow the guidelines and use the template hereinbelow to fill in any information.

To edit the document, please SAVE AS NEW DOCUMENT and follow the below naming convention:

[NAME OF PARTNER]_Task11.3_Partners Fill-In Form_version [1]

Name of Partner	
------------------------	--

Name of technology you lead:	
Date:	

Table of Contents

1. SWOT Analysis
2. Benefits to the Economy
3. Policy Plans & Regulatory Framework
4. Technological Trends
5. Key Innovative Technology - Comparison Criteria
6. Competitive Landscape

1. SWOT Analysis

Description: The SWOT (Strengths, Weaknesses, Opportunities, Threats) matrix is a tool to support strategic decision-making and help build a successful market access strategy for your product/service.

How to fill-in your SWOT matrix:

- Always keep in mind your objective, i.e. to commercialise your product/service.

The template must be filled from this point of view:

- What are the strengths for your product/service commercialisation? What are the opportunities for your product/service commercialisation? Etc.;
- Distinguish between internal factors (that come from your company, your products, your know-how etc.) and external factors (that come from your environment, competitors, laws & regulation, market trends etc.).

To work out if something is an internal or external factor, ask yourself if it would exist even if your business didn't.

- Rely on facts, not intuitions;
- Provide figures each time it is possible;
- Priorities.

Remain synthetic in the matrix and bring explanations below it if necessary (An external reviewer should be able to understand the foundation of your statements).

For more information on how to perform a SWOT analysis, please look at: https://www.mindtools.com/pages/article/newTMC_05.htm

Please use this template to fill in the SWOT analysis for each TESTUDO innovative technology.

	Name Service/Asset (XXX)	
	Favourable Factors	Adverse Factors
Internal Factors	Strengths <i>What do you do well?</i> <i>What unique resources can you draw on?</i> <i>What do others see as your strengths?</i>	Weaknesses <i>What could you improve?</i> <i>Where do you have fewer resources than others?</i> <i>What are others likely to see as a weakness?</i>
External Factors	Opportunities <i>What opportunities are open to you?</i> <i>What trends could you take advantage of?</i> <i>How can you turn your strengths into opportunities?</i>	Threats <i>What threats could harm you?</i> <i>What is your competition doing?</i> <i>What threats do your weaknesses expose you to?</i>

	Name Service/Asset (XXX)	
	Favourable Factors	Adverse Factors
Internal Factors	Strengths	Weaknesses
External Factors	Opportunities	Threats

2. Benefits to the Economy

Please provide us with information on what benefits to the economy your innovation/technology brings about. [100 words, in paragraphs]

You can focus on questions such as:

Why investing in such technologies will benefit the economy?
Who will gain from utilizing this technology? How will this benefit manifest?
How will these technologies bring about substantial - beneficial changes to their respective markets/industries?

3. Policy Plans & Regulatory Framework

In this Section, we ask you to provide information on any applicable laws that govern your technology in question. Laws governing the technology could be focused on matters such as:

- (i) technical specifications,
- (ii) limitations on utilisation and use of the technology,
- (iii) registration and/or licensing required for the technology, etc.

We are focused on 2 legal frameworks, namely:

1. *National/EU policy plans supporting/promoting utilisation of such technologies*
 - *EU regulations/directives:*
 - *National law different from EU law? If yes, how?*
2. *Third countries/beyond Europe:*
 - *USA*
 - *Australia*
 - *Other?*

Please provide the following information for each legal framework:

[100-500 words in each legal framework section, in paragraphs, with different subsections for Points 1 and 2 as above]

- Name of applicable law
- Brief description of law
- Impact of law on TESTUDO technology
- Web link access to law

[type here]

4. Technological Trends

Please provide the information with references (web links to publications/articles). [100-500 words, in paragraphs]

Why is there a move towards utilisation of this technology?
Which industries would benefit the most from the use of this technology?
What is the current market growth for this technology?
What are the current uses and what could be future uses of the technology?
Have major economic/financial/industrial and/or geo-political actors taken any steps towards utilising/developing/regulating the technology?

5. Key Innovative Technology - Comparison Criteria

It is essential to properly identify your solution comparison criteria, as they will allow you to benchmark your solution against competing ones, to highlight your competitive advantages and to help you define your unique value proposition to the prospective owners/operators.

How to identify your solution comparison criteria:

- Your solution comparison criteria must be as common as possible to all competing solutions.
- They should reflect the main technical and/or functional characteristics of the solution and the main investment and exploitation issues at stake.
- They should be customer-oriented i.e. they should be defined regarding customers' use cases, their needs and their constraints (financial, technical, skills related etc.).
- They should be adapted to your customers' profiles. If your customers are very technical, you should foster technical criteria. If not, you should foster functional ones.

The template table provided below will assist you in structuring your comparison criteria. Fill in the relevant fields accordingly.

Lead Partner	Pilot Technology	Technical Criteria	Functional Criteria	Commercial Criteria

6. Competitive Landscape

In the Competitive Landscape Section, you are asked to compile a list of relevant competitive technologies.

The first question on competition intensity is aimed at creating a general image of the competition within the industry. It is based upon Michael Porter's "Five Forces" strategy tool.

- Competitive Rivalry**
How many rivals do you have? Who are they, and how does the quality of their products and services compare with yours?
- Supplier Power**
How many potential suppliers do you have? How unique is the product or service that they provide, and how expensive would it be to switch from one supplier to another?
- Buyer Power**
How many buyers are there, and how big are their orders? How much would it cost them to switch from your products and services to those of a rival? Are your buyers strong enough to dictate terms to you?
- Threat of Substitution**
A substitution that is easy and cheap to make can weaken your position and threaten your profitability.
- Threat of New Entry**
How easy is it to get a foothold in your industry or market? How much would it cost, and how tightly is your sector regulated?

For more information on Porter's "Five Forces", please follow this link: https://www.mindtools.com/pages/article/newTMC_08.htm

For each pilot technology, the competitive landscape should be assessed and drafted and 3 relevant competitors should be included, as per the template herein below:

What is the competition intensity?	
1. <i>Competitive rivalry</i>	
2. <i>Supplier power</i>	

3. <i>Buyer power</i>	
4. <i>Threat of new entry</i>	
5. <i>Threat of substitution</i>	

Competitor 1:

--

Does this competitor have the same solution as you?:

--

Does this competitor have the same customers as you?

--

What are the limitations of this company compared to your solution?

--

Describe the performance of this company compared to your solution?

--

Can you point out how you are better or different (e.g. price, product size, market experience, innovation & new product, value, branding)?

--

Annex 2 – Key innovative technologies

The table below outlines the key innovative technologies, along with details about pilot technology, technical, functional and commercial criteria that partners develop and utilize in TESTUDO. These details will assist us in strategic planning and customer relationships analysis for the next Market Analysis in D12.2.

Lead Partner	Pilot Technology	Technical Criteria	Functional Criteria	Commercial Criteria
CERTH	3D mapping of CI from visual data	Deep-Learning algorithm	Offline procedure Aerial images from drones as input Point-cloud as output	AI-based technology Fast and semi-automated geo-referencing Drone data capture Time and cost effective solution
CERTH	Thermal detector and localizer module	A Multispectral detection module that will rely on AI-models using thermal/IR cameras to maximize surveillance capabilities during night and low-visibility weather conditions	The module consists of (i) input module, (ii) detection model (iii) result release component. Component (i) will collect the ways of collecting the thermal/IR data from the system and feed them to the (ii) component, which will analyse and estimate the presence of objects of interest. Component (iii) will release the detection outcomes to the system in a manner that could be exploited by other TESTUDO services.	Robustness and Reliability: The module will deliver a 24/7 detection service and ensure operations under diverse weather condition that affects the capacities of visual cameras. Regulatory Compliance: the module will comply with EU standards, regulations and related legislation. Integration Capabilities: The module will integrate with other TESTUDO services and modules for advance processing and decision making.
CERTH	Automatic object detection and identification from visual spectrum	Deep Learning object detection model	Real-time detection for improved decision-making	Customizable object detection tool Adaptation to various object categories based on buyers' needs Ensure high performance under real-world conditions
CERTH	Event predictor module	The module will create Digital replicas of CIs by	The module consists of the following components:	The module will deliver a decision making framework that will operate on the digital world to

		<p>using 3D representation schemas coming from other TESTUDO components and simulating the results of virtual stimulations. It will analyse detection outcomes and raw/fused data to provide predictive insights for the decision-making process. The developed DTs will retain the system's operators in the loop for safety reasons, by assessing the event/situation and its threat assessment, sharing the decision with the existing infrastructure and re-assessing the event/situation.</p>	<p>(i) input module, (ii) simulation module (iii) decision making framework component. Component (i) will establish an interconnection with modules that provide all the necessary data about the operational condition of the assets and feed them to the (ii) component which will deploy AI-based architectures for prediction analysis. Component (iii) will operate in the digital world to assess the evolution of a potential decision provided by the operator of the TESTUDO system.</p>	<p>assess the evolution of a potential decision provided by the operator.</p> <p>The module's reliability will be tested in operational and pilot demonstrations that will take place in the relevant facilities.</p> <p>Integration Capabilities: The module will be capable of exchanging data with other TESTUDO components for advance processing and decision making.</p> <p>Regulatory Compliance: the module will comply with EU standards, regulations and related legislation.</p>
ACCELI	CERBERUS and DIOPTRA UAVs	<p>Open source: Software with source code that anyone can inspect, modify and enhance. Algorithms utilised GPU support: Embedded AI-driven operation for enhanced decision support capabilities UAV neutralization: Automation of the overall procedure with no "time to react" delays.</p>	<p>Detection, Recognition, Alarm for any approaching threat Mission UAV can approach the object and identify the situation Onboard sensors and cameral for ship surveillance and nearby areas.</p>	<p>User-friendly: easy to be used by anyone with minimal training Ecosystem friendly Continued technical support and updates.</p>

		Perform image/video processing. Threat detection and forecasting: using advance anomaly-based detection models to indicate deviations to normal system activity w.r.t. The application and signify potential threats before they cause critical damage.		
STWS	ENGAGE CSIM platform (T8.4-9.4 Monitoring centre with improved HMI via DTs and XR technologies)	-Integration Capabilities -Scalability and Performance - Interoperability - Data Analytics and Correlation - Real-Time Monitoring and Alerting	-Incident Management -Response plans and workflow automation - Compliance and Reporting -User friendliness and UI -customization -UI and access to data per role defined by the entity	- Total Cost of Ownership - Deployment Options - Contractual Terms and SLAs
CEA	SigmoIDS	High detection accuracy	Real-time intrusion detection Dynamic response identification Adaptability to various communication protocols	Flexibility Ease of deployment
T4i	Upgraded T4i DOVER®	Weight: 18.-2.5kg A built-in calibrator module will be included provided a continuous calibration for qualitative measurements Fast conversion from hand portable	Real time detections of target vapours Transmission of alarms to the operational centre Addressing ambient environment changes (pressure, temperature, humidity)	Reliability Remote detection Fast maintenance Well- trained operators

		to airborne instrument	Fast and miniaturised chemical detector	
T4i	T4i FemtoMachine®	Weight: 2.5kg [Included batteries] Hand portable for use indoors and outdoors Does not use dangerous and costly gas cylinders. Air ambient is used Broad range of TICs and env. VOCs, CWAs and explosives simulants	User-friendly GUI Communication Interface: USB Oven warm-up:30 mins Oven accuracy: 0.1°C Output flow repeatability:1%	There is no great competition due to the fact that T4i FemtoMachine a portable device. It is standardized: CE, RoHS, ISO EN 6145-10:2019, IPC-A-610
VICOM	Activity Recognition and Explainable AI	Detection of activities and threats in the context of TESTUDO Explainable AI following the requirements establish in the project	Increase the capabilities to analysis AI models and increase their resistances to attack Identify a number of key visual situations which put in danger CI.	Ecosystem friendly Tailored to the CI environment and limitations
SINTEF	Autonomous resource allocation algorithms		Able to incorporate different types of mobile sensor platforms. The use of mobile assets will consider placement of fixed sensors. Ability to optimize overall surveillance coverage when multiple mobile sensor platforms are used.	More efficient use of the available mobile sensor platforms than is realistic to achieve with manual methods.
DFKI	ASGUARD IV Unmanned Vehicle	Size: 935mm x 560mm x 500mm) Weight: 16Kg Power supply: Lithium Polymer Batt. 4 x Kokam 15V 5000mAh	Small and light weight Good all terrain capabilities Fast and agile High payload capacity	Low maintenance cost through relative simple and robust design Low cost if mass-produced Flexible configuration possible

		<p>Motors: DC-Motor: Faulhaber 3863 024 CR + Planetengetriebe 66:1</p> <p>Sensors: 360° Laser Scanner: Velodyne 32 Lidar</p> <p>- Stereo camera: 2 x Entaniya Fisheye 220</p> <p>- IMU: Xsens Mti-28A53G35</p> <p>- Optic increm. encoder Agilent AEDB-9140</p> <p>Comm. : Mobile Router: ASUS WL-330N3G, Long Range radio RF Modem: AMBER Wireless AMB8385</p> <p>Computer: Embedded PC Quad Core i7</p>	Remote controlled or autonomous	
TEK	Edge computing	<p>offers reduced latency</p> <p>Assessment of power consumption and operational efficiency</p>	<p>increased reliability</p> <p>enhances real-time decision-making</p>	Non reliance on commercial servers
ADS	HASP			

Annex 3 – Benefits to the Industry, Market Players and to the Economy

– Contributions from partners

Partner Acronym	Comment
CERTH	<p>Three-dimensional representations of geometric data:</p> <p>A precise 3D model of a CI/public space combined with Digital Twin technology provides a digital mirror image of the physical entity playing a crucial role in enhancing security, safety, and resilience. By providing real-time situational awareness, threat detection, and response capabilities, these technologies help mitigate risks, prevent disruptions, and ensure continuity of essential services, thereby safeguarding economic activities and societal well-being.</p> <p>In the context of the TESTUDO project, CI operators will primarily benefit from 3D mapping technology for enhanced site monitoring and improved decision-making efficiency. These maps offer detailed insights into building layouts, access points, and other relevant information, supporting CI operators to plan and coordinate their actions more effectively and reduce response times in emergency situations. Beyond the CI sector, 3D mapping holds potential applications in urban planning, the construction sector, and various agricultural applications.</p> <p>In CI management 3D mapping technologies play a crucial role in enhancing safety and resilience by providing real-time situational awareness, accurate threat assessments, and effective emergency planning and response capabilities. Moreover, accurate and precise 3D maps provide operators with valuable insights and information, enabling more informed decision-making.</p> <p>Event Predictor:</p> <p>Investing in technologies like the "Event Predictor" module can enhance the capabilities of a monitoring centre in a CI. To this end, situation awareness, operational efficiency, and decision-making processes are expected to be improved. This translates to reduced downtime, enhanced security, and optimized resource allocation, bolstering the reliability and resilience of essential infrastructure systems. In turn, these advancements stimulate economic growth by safeguarding investments, increasing productivity, and fostering innovation, thereby fortifying the foundation for sustained prosperity in various sectors of the economy.</p> <p>In TESTUDO, utilizing the module as a component of a CI monitoring centre benefits operators, security personnel, and decision-makers for optimal surveillance. The technology offers an advanced prediction service, providing these stakeholders with enriched situational awareness and streamlined decision making framework. This manifests as quicker threat identification, more informed decision-making, and improved responses to events. Ultimately, it empowers individuals overseeing critical infrastructure, ensuring a safer and more efficient operation, reducing risks, and safeguarding assets, thereby benefiting both the personnel responsible for infrastructure security and the broader community relying on these vital systems.</p> <p>Predictive analysis models can elevate surveillance efficiency, threat early identification, and decision-making processes for CI protection domain. This leads to a paradigm shift in operational efficiency, risk management, and decision-making within critical infrastructure sectors. The integration of predictive analysis, digital twins, in complement with advanced HMIs, ensures quicker response times, reduced downtime, and increased resilience. These significant improvements not only increase the security and</p>

Partner Acronym	Comment
	<p>reliability of critical infrastructure and their smooth operations, but also set new standards for efficiency and safety, initiating positive changes and advancements in their respective markets, ultimately shaping more robust and technologically advanced industries.</p> <p>Thermal detector and localizer:</p> <p>Enhanced capabilities in multispectral scanning contribute to safer environments, protecting critical infrastructure and public spaces and avoiding potential damage that may require significant repairs. Hence, saving of funding resources and their investment in other domains is applicable. This technological investment not only stimulates the tech sector but also improves overall national security, positioning Europe at the forefront of cutting-edge advancements in surveillance technology.</p> <p>Within the scope of TESTUDO project, the CI operators can improve their security measures, reducing the risk of breaches or attacks. Beyond the CI domain, law enforcement can benefit from enhanced surveillance capabilities for crime prevention and detection. Security agencies can also gain from improved monitoring of sensitive areas, borders, and critical infrastructure. Overall, the technology leads to safer environments, reduced losses, and increased efficiency in operations, manifesting in lowered crime rates, improved emergency response, and protected critical infrastructure.</p> <p>In the surveillance market, the Thermal Detector and Localizer will set a new benchmark for low-visibility detection, expanding applications in CI protection. These modules can enhance perimeter protection and asset security, reducing risks and losses. In addition, security industry, law enforcement, and transportation and utilities industries that need reliable surveillance will experience heightened safety and efficiency, reducing downtime and losses.</p> <p>Automatic object detection and identification from visual spectrum:</p> <p>Automatic object detection technology contributes to increased CI security and safety by helping to identify potential threats. By investing in this technology, CI operators and governments can more efficiently protect these sites, reducing the economic impacts of criminal activity. Moreover, the adaptation of these technologies by businesses makes them more competitive, increasing their productivity and decreasing their costs through more efficient resource allocation.</p> <p>In the specific context of the TESTUDO project, both public and private CI operators will benefit from the utilisation of automatic visual object detection, achieving more efficient and effective surveillance and monitoring of their premises under real-world conditions. Beyond the CI sector, this technology, with the necessary adaptations, could be exploited in the context of a smart city for monitoring and data analysis, in healthcare for medical imaging, and in border management.</p> <p>In sectors such as CIs, defence, law enforcement and public security, visual object detection technologies offer more efficient security solutions. By accurately identifying and tracking objects of interest, these technologies could prevent security breaches, detect potential threats, and support security personnel to respond to incidents in a timely manner. This leads to safer environments for businesses, governments, and individuals, ultimately boosting confidence and trust in the market.</p>
ACCELI	Investing in advanced unmanned aerial vehicle (UAV) technologies, exemplified by platforms like CERBERUS and DIOPTRA, offers significant economic advantages. These cutting-edge UAVs, tailored for specific

Partner Acronym	Comment
	<p>missions and equipped with high-performance sensors, bring unparalleled capabilities to diverse sectors. Take, for instance, critical infrastructure surveillance. CERBERUS, an octa-rotor UAV, and DIOPTRA, an electric tailsitter fixed-wing UAV with VTOL characteristics, are designed to optimize inspection processes. Their advanced imaging and sensing payloads, such as the Flir Duo Pro R HD Dual-Sensor Thermal Camera and MicaSense RedEdge-MX multispectral camera, enable streamlined inspections, minimize downtime, enhance security, and contribute to cost savings through early detection of issues. Moreover, the integration of these UAV technologies, with their precision automated take-off/landing and autonomous flight features, not only addresses immediate infrastructure needs but also fuels job creation, fosters innovation, and triggers economic growth across various related industries.</p> <p>The utilization of advanced UAV technologies, exemplified by platforms like CERBERUS and DIOPTRA, offers multifaceted benefits to various stakeholders. In the specific context of critical infrastructure surveillance, including monitoring water dams, the gains are substantial. Infrastructure operators deploying CERBERUS and DIOPTRA experience increased reliability and cost savings through proactive UAV-based inspections, thanks to the advanced capabilities of sensors like the Flir Duo Pro R HD and MicaSense RedEdge-MX. Governments benefit from enhanced security and reduce economic burdens associated with emergency repairs, leveraging the precision automated take-off/landing and autonomous flight features of these UAVs. The public, in turn, enjoys the broader advantages of resilient and safe critical infrastructures, ensuring uninterrupted services and minimizing the potential impact of infrastructure failures on daily life.</p> <p>The integration of advanced UAV technologies, exemplified by platforms like CERBERUS and DIOPTRA, heralds transformative and beneficial changes across diverse markets, with a particular focus on critical infrastructure. In the realm of water dam surveillance, the adoption of these UAVs is becoming imperative for efficient and reliable monitoring. This evolution not only creates new opportunities for UAV manufacturers and service providers but also catalyzes innovation in sensor technologies, data analytics, and aerial surveillance techniques. CERBERUS, with its octa-rotor design and the powerful NVIDIA Jetson AGX Xavier AI-oriented computer, and DIOPTRA, as an electric tailsitter fixed-wing UAV with VTOL characteristics, lead the way in driving advancements. These progressions contribute to a more sophisticated and interconnected market ecosystem, establishing UAVs as indispensable tools for ensuring the longevity, safety, and economic efficiency of critical infrastructure.</p>
STWS	<p>Robust security measures provided by CSIM solutions improve business resilience and continuity, enabling organizations to respond effectively to security threats and disruptions. In this direction, less financial resources will be spent by CI operators, governments & organizations for crisis management and impact mitigation/damage repair. Resources saved can be used for the CIs or a country's growth. By reducing the consequences of cybercrime or physical attacks, different entities unlock future economic value, as higher levels of trust encourage more business from customers. The companies/operators will benefit by reaching a stronger position in the market and by expanding their customer portfolio.</p> <p>Investing in CSIM systems benefits the economy by enhancing security infrastructure, stimulating innovation, and creating job opportunities. CSIM investments foster industry growth and competitiveness, driving revenue growth for technology vendors and solution integrators.</p>

Partner Acronym	Comment
	<p>The main stakeholder that will benefit from such technology is that of CI operators, while a significant benefit may concern public and private authorities that are involved in incident management of a CI. Indirect benefits may occur also to the society, as citizens and organizations are protected while maintaining the feeling of safety and security.</p> <p>CSIM technologies bring substantial beneficial changes by revolutionizing security operations, streamlining processes, and mitigating risks. They offer comprehensive integration of security systems, enabling real-time monitoring, advanced analytics, and automated responses to threats. This enhances situational awareness, improves incident response times, and reduces operational costs. CSIM solutions also facilitate compliance with regulatory requirements, bolstering trust and confidence among stakeholders. By providing scalable, adaptable, and proactive security measures, CSIM technologies drive innovation, competitiveness, and resilience across various sectors, ultimately safeguarding assets, data, and operations in an ever-evolving threat landscape.</p>
CEA	<p>Efficient intrusion detection and response are paramount for ensuring the resilience of network-based services. Timely detection and response to cyber-attacks limit unexpected service interruptions and prevent large-scale damage that undetected intrusions may inflict. Investing in SigmIDS potentially saves companies from significant monetary losses caused by novel cyber threats for which signatures are not yet available.</p> <p>Any company or institution endowed with an intra-network, or even owning a simple router, is a potential target for cyber threats.</p> <p>Networks with regular traffic flows will benefit the most from it, as the likelihood of having false alerts is significantly reduced for these.</p> <p>SigmIDS will demonstrate its benefits by avoiding unexpected service disruptions or data leaks.</p> <p>Most commercially available IDS rely on rule-based intrusion detection. While this is an important component of any IDS, it can only capture known cyber threats. On the other hand, SigmIDS has the capability of detecting novel attacks by observing anomalies in the network traffic.</p>
T4i	<p>T4i DOVER® (upgraded):</p> <p>Chemical detectors mounted on UAVs, like T4i DOVER®, streamline monitoring and surveillance processes by providing real-time data collection and analysis. This enhanced efficiency translates into cost savings for industries such as agriculture, environmental monitoring, and infrastructure inspection, like water dumps, where timely detection of chemical hazards is critical for decision-making and risk management. Moreover, mounted chemical detectors play a crucial role in safeguarding public health, environmental quality, and infrastructure integrity by detecting and monitoring chemical pollutants, leaks, and hazardous substances. Proactive detection and mitigation of chemical hazards contribute to reducing the risk of accidents, minimizing environmental damage, and enhancing overall safety standards, thereby reducing associated economic costs.</p> <p>Various stakeholders stand to gain from utilizing advanced chemical detection technologies for UAVs, like T4i DOVER®. T4i DOVER® excels in offering real-time monitoring capabilities, particularly crucial during emergency events. This technology not only enhances operational efficiency but also significantly improves</p>

Partner Acronym	Comment
	<p>response capabilities, underscoring its substantial impact on ensuring safety and security across diverse applications such as critical infrastructures surveillance, environmental monitoring, defence, industrial safety, maritime security& safety as well as government agencies responsible for security and regulatory compliance.</p> <p>Chemical detectors being mounted on UAVs, like T4i DOVER®, will bring about substantial beneficial changes to their respective markets and industries by enabling remote, reliable and efficient detection of chemical substances, early warning systems for environmental hazards, enhanced security measures, and improved regulatory compliance. This will lead to increased competitiveness, improved operational efficiencies, and better risk management practices, ultimately driving positive economic and societal outcomes within these sectors.</p> <p>T4i FemtoMachine®:</p> <p>Investing in technologies like portable vapor generators and calibrators benefits the economy in several ways.</p> <p>Increased productivity: Streamlined processes and improved efficiency lead to higher output per unit of input, driving economic growth.</p> <p>Innovation and competitiveness: Investment in innovative technologies fosters growth and helps businesses stay competitive in global markets.</p> <p>Environmental sustainability: Technologies that improve efficiency contribute to sustainable development goals, enhancing long-term economic stability and resilience.</p> <p>Various stakeholders stand to gain from the utilization of these technologies:</p> <p>Sensors and instrumentation industries: Improved efficiency, productivity, and quality control lead to cost savings and enhanced competitiveness.</p> <p>Regulatory bodies: Accurate measurements and compliance with standards lead to better regulation and oversight, ensuring public safety and environmental protection.</p> <p>Customers: Field used products and services result in better outcomes and experiences for customers in QA/QC in the field.</p> <p>The use of vapour generators that can act as calibrators like T4i FemtoMachine® enable more reliable measurements, enhanced efficiency, and increased QA/QC in the field.</p>
VICOM	<p>The aim is to transfer technologies to enable businesses to be more competitive and to have a positive impact on society, in line with our social commitment.</p> <p>The inclusion of these technologies will facilitate the process of monitoring and protecting CI.</p> <p>This process could then be transferred to a general variety of areas like industry, smart city, etc. These areas will benefit from the real-time analytics of our system.</p>

Partner Acronym	Comment
SINTEF	<p>Autonomous resource allocation algorithms can contribute to enhanced public safety by providing a more optimal surveillance coverage and thus improve the protection of assets and infrastructure. By enabling efficient analysis of large volumes of data and the detection of security threats in real-time, these algorithms enable faster response times, minimizing the impact of security incidents on businesses and communities. Enhanced security measures can attract investment and support economic development. Additionally, the implementation of effective surveillance algorithms can lead to cost savings by reducing the need for manual monitoring and increasing the efficiency of security personnel.</p> <p>Utilizing autonomous resource allocation algorithms enhances security for critical infrastructure where multiple mobile robots/platforms are available, benefiting government agencies, operators, security firms, technology providers, and society at large. These algorithms optimize resource deployment, bolstering preparedness, efficiency, and resilience. They integrate diverse data sources for heightened situational awareness, enabling rapid threat response and minimizing downtime. By automating decision-making and response actions, they reduce response times and mitigate security risks. Overall, they contribute to a resilient security architecture, safeguarding essential services, public safety, and national security.</p> <p>Autonomous resource allocation algorithms for critical infrastructure protection can provide substantial beneficial changes by optimizing the allocation of resources such as personnel, equipment, and technology to safeguard vital assets. The algorithms receive real-time information about vulnerabilities and risks, and prioritize protective measures, ensuring efficient deployment of resources where they are most needed. By enhancing the resilience of critical infrastructure against threats such as natural disasters, and physical sabotage, these algorithms minimize downtime, reduce economic losses, and safeguard public safety, ultimately fostering greater stability and confidence in essential services and systems.</p>
DFKI	<p>Small and fast robotic rovers, such as the ASGUARD IV, offer economic benefits through cost efficient deployment, efficient data collection capabilities, relative low investment needs, and low maintenance costs. Compared to the installation of fixed sensors, the deployment of sensors on a mobile platform such as ASGUARD IV offers significant savings, in particular in the case of expensive sensors.</p> <p>Gains from using this technology can be made in particular by stakeholders owning and operating critical infrastructures or by companies providing inspection services to those infrastructure owners. This refers to private company as well as to public and governmental organizations, such as fire brigades, rescue services, technical disaster managers, police and security forces.</p> <p>The benefit will manifest in increased capabilities for inspection of critical infrastructure and a decrease in the risk involved to the human staff involved in these inspections.</p> <p>Small, easy-to-use mobile robots can access tight spaces and hard-to-reach areas, and navigate complex environments more efficiently than traditional methods. Mobile robots are a cost-effective alternative to traditional inspection methods. They can lower overall inspection costs while maintaining or improving the quality of data collected.</p> <p>Small mobile robots are capable of conducting inspections more quickly than human inspectors or larger robotic systems. Mobile robots can cover large areas quickly, reducing disruptions to operations and downtime for critical infrastructure. They also enhance safety by reducing the risk of accidents and exposure to dangerous conditions. Mobile robots can collect data on infrastructure components. They can also be</p>

Partner Acronym	Comment
	<p>used for remote monitoring of critical infrastructure assets. This lets operators fix problems before they become expensive or cause problems.</p> <p>The modular design and scalability of mobile robot systems let them do a wide range of inspections in different places. They can be easily changed to suit different inspections.</p> <p>Small, easy-to-deploy mobile robots could change the market for critical infrastructure inspection. They could be more cost-effective, efficient, and safer than traditional methods. They could also enable more proactive maintenance and management strategies.</p>
TEK	<p>TEKNIKER's technology contributes to enhanced infrastructure safety, potentially reducing the economic impact of catastrophes.</p> <p>The low-cost nature of the platforms encourages widespread adoption, benefiting public and private sectors. Critical infrastructures, smart city initiatives, autonomous vehicles, manufacturing or healthcare will greatly benefit from edge computing technology.</p> <p>Advances in edge AI could stimulate local technology sectors and job creation. These sectors will benefit from the low latency, real-time analytics, and improved efficiency that edge computing offers.</p>
ADS	<p>Investing in High Altitude Platform Station (HAPS) technology will benefit the economy in several ways:</p> <ol style="list-style-type: none"> 1. **Economic Growth**: HAPS technology can bridge the digital divide, providing internet access to underserved areas, which can lead to increased economic growth and social development. 2. **Cost-Effective Deployment**: Compared to traditional infrastructure or satellite systems, deploying HAPS is more cost-effective, making it an attractive option, especially in remote areas with limited resources. 3. **Flexibility and Mobility**: HAPS can be easily deployed and relocated to areas with specific connectivity needs, providing targeted coverage and supporting disaster-stricken regions or temporary events. 4. **Extended Coverage**: HAPS can provide coverage to vast geographical areas, including regions where laying cables or implementing ground-based infrastructure is challenging or not economically feasible. 5. **Rapid Deployment**: Unlike traditional infrastructure setup, HAPS can be deployed relatively quickly, reducing the time required to establish connectivity in underserved areas. 6. **Environmental Sustainability**: Compared to traditional satellite-based communication systems, HAPS offer a more sustainable solution, requiring less power consumption, emitting lower carbon emissions, and having a longer lifespan. 7. **Enhanced Data Transmission**: Leveraging HAPS can optimize operations through real-time monitoring, remote expert support, and efficient planning, ultimately improving efficiency and reducing costs. 8. **Increased Investment in High-Tech Industries**: The growing demand for high-altitude platforms in various industries, such as oil and gas, telecommunications, and aerospace, will lead to increased investment in high-tech industries, fostering innovation and job creation.

Partner Acronym	Comment
	<p>9. **Improved National Security**: Governments are investing in high-altitude platforms for defence and military purposes, which can lead to improved national security and strategic advantages.</p> <p>10. **Technological Advancements**: The development of high-altitude platforms will drive technological advancements in various sectors, such as communication, surveillance, and environmental monitoring, leading to further economic benefits.</p> <p>In conclusion, investing in HAPS technology will not only benefit specific industries but also contribute to overall economic growth, job creation, and technological advancements, ultimately enhancing the competitiveness of the global economy.</p> <p>Utilizing High Altitude Platform Station (HAPS) technology will benefit various stakeholders and industries, leading to tangible advantages:</p> <ol style="list-style-type: none"> 1. **Oil and Gas Industry**: Oilfield operators will gain from improved safety, enhanced coordination, and optimized operations through real-time monitoring, remote expert support, and efficient planning facilitated by HAPS technology. This will result in increased efficiency, reduced costs, and better environmental monitoring, ultimately transforming the industry's communication infrastructure. 2. **Telecommunications Industry**: Companies like Airbus, Thales Group, and HAPSMobile are at the forefront of HAPS technology development. The telecommunications sector will benefit from extended coverage, reliable connectivity, cost-effective solutions, and quick deployment capabilities offered by HAPS. This technology will enable seamless communication in remote areas with limited infrastructure, driving economic benefits and enhancing connectivity. 3. **Aerospace Industry**: The HAPS Alliance aims to accelerate the commercial adoption of HAPS technologies in the stratosphere. By promoting high-altitude platforms, the aerospace industry will witness advancements in communication technologies, environmental monitoring capabilities, and sustainable solutions. This collaboration will lead to increased investment in high-tech industries and foster innovation within the aerospace sector.. 4. **Environmental Sustainability**: Utilizing HAPS technology offers a more sustainable alternative to traditional satellite-based communication systems. With lower power consumption, reduced carbon emissions, and longer lifespan, HAPS contribute to environmental conservation efforts while providing reliable connectivity for various industries. 5. **Global Connectivity**: The HAPS Alliance's vision is to eliminate the digital divide by bringing connectivity to more people worldwide through the accelerated promotion of high altitude platform stations (HAPS). This initiative will enhance global connectivity, bridge communication gaps in underserved areas, and drive economic growth through improved access to information and resources. <p>In summary, stakeholders across industries such as oil and gas, telecommunications, aerospace, and environmental conservation stand to gain significantly from utilizing HAPS technology. The benefits include improved safety measures, enhanced operational efficiency, cost-effective solutions, sustainable alternatives, global connectivity advancements, and increased investment in high-tech sectors.</p>

Partner Acronym	Comment
	<p>High Altitude Platform Station (HAPS) technology is poised to bring substantial beneficial changes to various markets and industries. Some of the key advantages and potential impacts of HAPS technology include:</p> <ol style="list-style-type: none"> 1. **Bridging the Digital Divide**: HAPS can extend internet access to remote and underserved regions, bridging the digital divide and unlocking new opportunities for education, commerce, and social progress. 2. **Rapid Deployment in Emergency Situations**: During natural disasters or emergency situations, HAPS can be rapidly deployed to restore communication networks, facilitating quick disaster response and saving lives. 3. **Enhanced Mobile Connectivity**: HAPS can act as floating base stations, complementing existing mobile networks, and extending coverage to rural areas where it is typically challenging to establish traditional network infrastructure. 4. **Environmental Sustainability**: Solar-powered HAPS offer an eco-friendly solution for expanding communication networks, reducing reliance on fossil fuels, and resulting in a smaller carbon footprint. 5. **Future Outlook**: The potential applications of HAPS are vast and promising. As the technology continues to evolve, we can expect significant advancements in the coming years. Industry forecasts estimate that by 2025, the HAPS market will reach a value of over \$1 billion, driven by increasing demand for enhanced connectivity and communication worldwide. 6. **Industry Growth**: The global 3 largest manufacturers of HAPS are Airbus, Thales Group, and HAPSMobile, which make up over 100% of the market[1]. The telecommunications industry is actively exploring partnerships and investments in high altitude platform technology, with giants like Google and Facebook already making substantial investments in developing their high altitude platform projects. 7. **Key Takeaways**: HAPS offer immense potential for bridging the digital divide and extending internet access to remote areas, providing a solution for enhancing mobile connectivity in rural areas, and promoting environmental sustainability. <p>In conclusion, the adoption of HAPS technology will benefit various stakeholders and industries, leading to tangible advantages such as improved safety measures, enhanced operational efficiency, cost-effective solutions, sustainable alternatives, global connectivity advancements, and increased investment in high-tech sectors.</p>

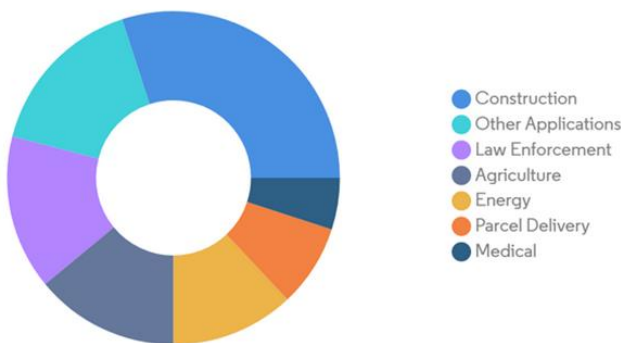
Annex 3 – Lists of current technology trends which are relevant to the innovations being developed in TESTUDO

UAVs

The commercial use of UAVs (drones) is rapidly expanding across various industries due to their efficiency, reliability, and cost-effectiveness. Key sectors benefiting from UAV and AI technologies include agriculture, energy, construction, media, maritime, security, and surveillance. This trend showcases the vast commercial potential of UAVs in supply chains within primary and secondary economies.

Market projections indicate that the European drone market will grow significantly.

Europe Drones Market: Revenue Share (%), by Application, 2021



Source: Mordor Intelligence



Figure 8. Europe Drone Market Revenue Share (2021).

UAVs are currently used for monitoring and mapping, providing a bird’s-eye view for faster, more efficient, and cost-effective project evaluations. In the maritime industry, UAVs help maintenance officers inspect ship hulls for leaks and damages without physical intervention, using advanced camera sensors to send clear images for assessment.

Three-dimensional representations of geometric data

3D maps provide a more immersive and detailed visualization of spatial environments compared to traditional 2D maps. They allow for better analysis and understanding of spatial relationships, which is particularly beneficial for security, defence, and emergency sectors in real-time incident response.

The technology has wide-ranging applications in industries such as CI monitoring, urban planning, construction, emergency response, and environmental monitoring. The 3D mapping and modelling market is expected to grow from \$6.77 billion in 2024 to \$22.19 billion by 2032, with a CAGR of 16%. Key

drivers of this growth include construction, urban planning, and infrastructure management, along with the adoption of VR, AR, and digital twins.

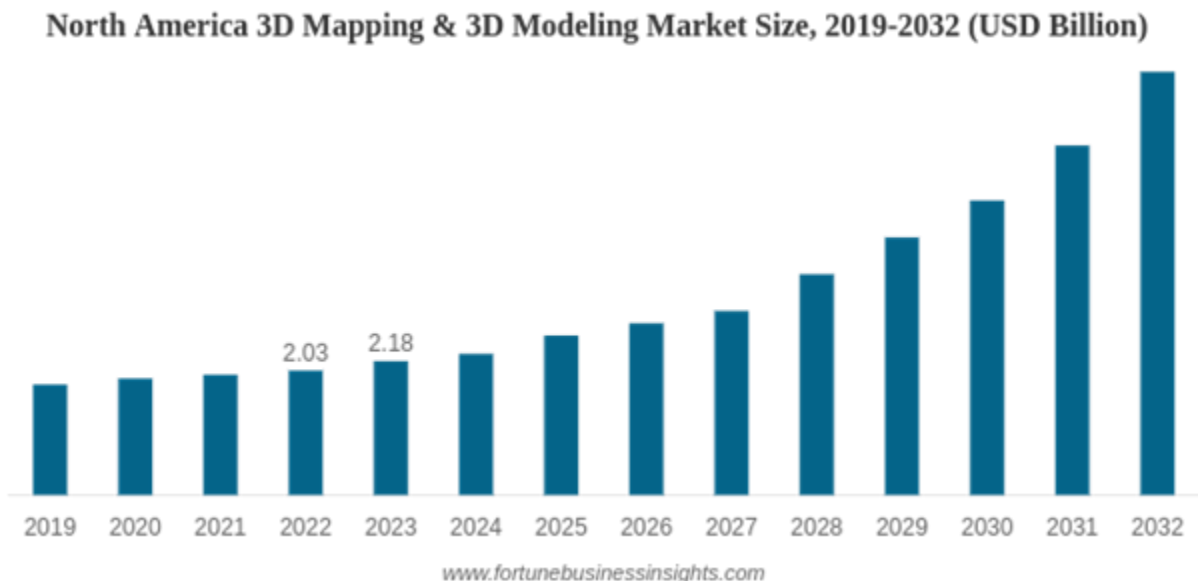


Figure 9. North America 3D Mapping & 3D Modelling Market Size, 2019-2032 (USD Billion).

Current applications of 3D mapping technology include CI monitoring and management, urban planning, environmental monitoring, building information modelling (BIM), and agriculture monitoring. Emerging uses involve creating digital twins, integrating with VR and AR platforms, and enhancing autonomous vehicle navigation and localization.

Private companies are investing in developing 3D mapping and modelling software, such as GIS mapping, drone mapping, and photogrammetry software. Research centres and institutions are also working on new methods and algorithms, including Deep Learning techniques, to improve the accuracy and efficiency of 3D modeling.

Thermal detector and localizer

The adoption of advanced surveillance technologies, such as the Thermal Detector and Localizer module, is increasing to enhance security measures in a rapidly evolving threat landscape. These technologies offer effective monitoring in challenging conditions, driven by the need for improved public safety, protection of critical infrastructure, and advancements in AI and sensor technologies.

Industries like law enforcement, security services, defence, and critical infrastructure sectors (transportation, energy, telecommunications) benefit significantly from these technologies. Precision agriculture also gains from multispectral cameras that provide detailed crop health information.

The global thermal imaging market, valued at USD 6.65 billion in 2022, is expected to grow to USD 14.02 billion by 2032, with a CAGR of 7.8%. Key growth drivers include increased government spending on aerospace and defence, and the adoption of advanced driver assistance systems across various sectors.

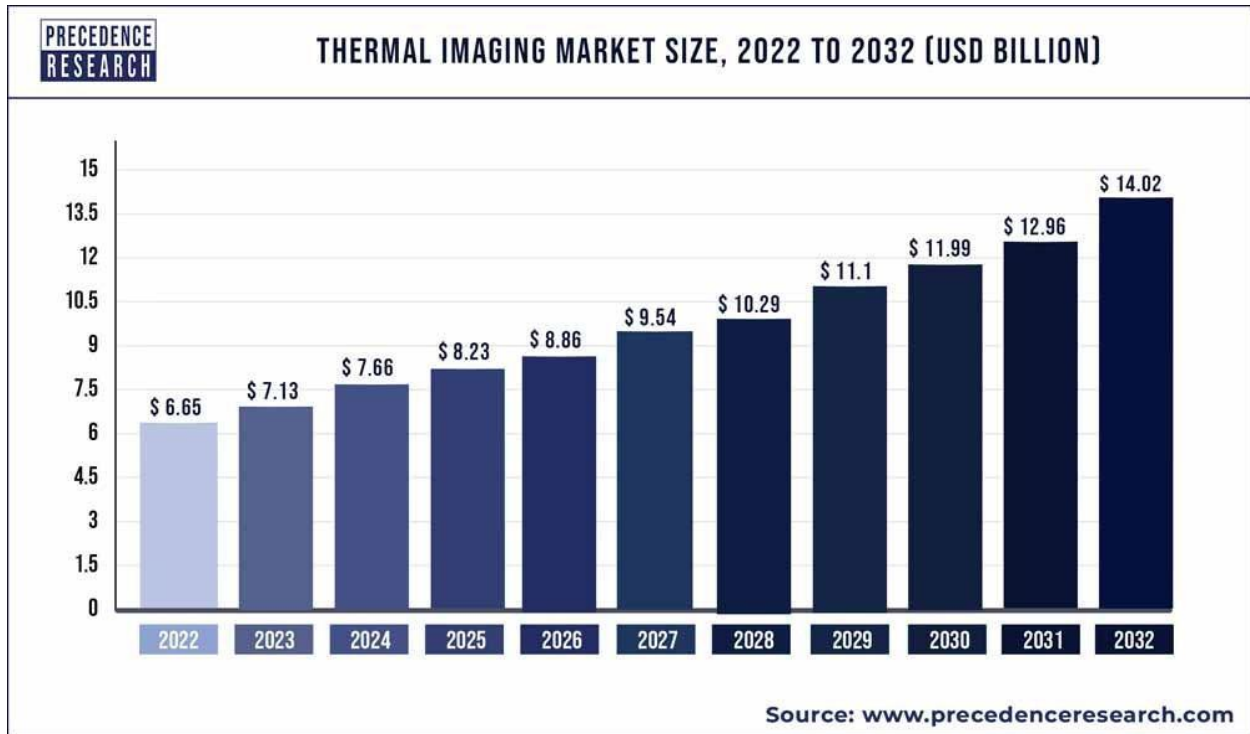
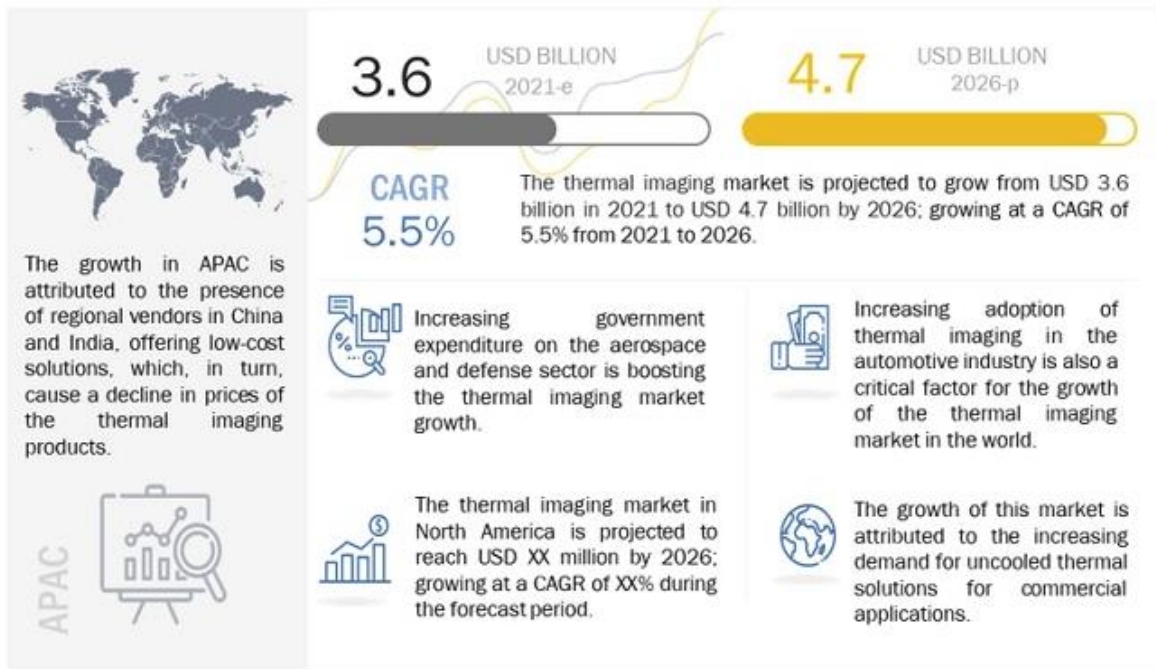


Figure 10. Thermal Imaging Market size, 2022 to 2032 (USD Billion).

Attractive Opportunities in Thermal Imaging Market



e-estimated, p-projected
© 2009 - 2021 MarketsandMarkets Research Private Ltd. All rights reserved

Figure 11 Attractive Opportunities in Thermal Imaging Market.

Advanced thermal imaging is in demand across various sectors, including healthcare, life sciences, manufacturing, defence, and military. Key market insights include:

- **Product Segment:** Handheld devices held a 64% market share in 2022 and are the fastest-growing segment due to their convenience.
- **Application Segment:** Security and surveillance accounted for 48% of revenue in 2022.
- **End User Segment:** Aerospace and defence captured around 39% of revenue in 2022.

Fixed thermal imaging devices are widely used in CCTV cameras for surveillance. Advanced driver assistance systems and the inclusion of thermography in healthcare present significant growth opportunities.

Governments, defence agencies, and law enforcement entities invest in advanced surveillance systems for national security. Private companies in defence and technology sectors are developing cutting-edge surveillance technologies. Many countries, including EU members, are implementing or considering regulations to govern the ethical use, data privacy, and potential abuses of surveillance technologies.

Automatic object detection and identification from visual spectrum

The adoption of visual object detection technology is driven by the need for advanced security solutions, advancements in AI and computer vision, automation, and demand for customized solutions. This technology benefits sectors like critical infrastructure, public security, defence, agriculture, healthcare, transportation, and infrastructure inspection.

The global image recognition market, valued at USD 45.02 billion in 2022, is expected to grow at a CAGR of 13.4% from 2023 to 2030. Image recognition, powered by machine learning, is being integrated into various fields.

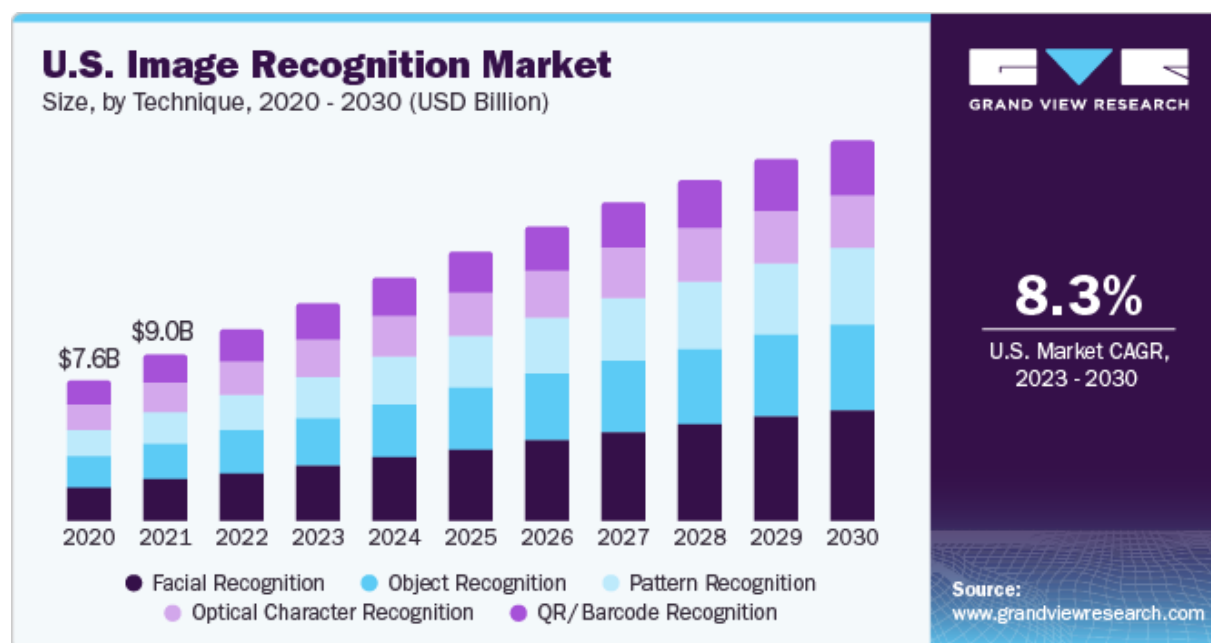


Figure 12 U.S Recognition Market.

Visual object detection is currently used for monitoring critical infrastructures, public spaces, threat detection, medical imaging, traffic management, and manufacturing inspection. Emerging applications include autonomous vehicles, robotics, augmented reality, and environmental monitoring. Companies like Google, NVIDIA, and Facebook, along with academic institutions, have been enhancing this technology by exploring new architectures, data types, and optimization methods. Both private and public security entities, including government agencies and military contractors, are investing in and regulating these technologies for security and surveillance purposes.

Event Predictor

Digital Twin (DT) technology replicates products, processes, or services in the digital space, providing feedback from the virtual world. It transforms the management of cyber-physical systems and promotes modularization to solve complex problems. AI in DTs is a rising trend in applications like product design, equipment manufacturing, surveillance, and aerospace. Prediction models enhance DTs by analysing

data, making predictions, and offering autonomous responses. In aerospace, defence, automotive, and assembly, nearly all physical designs can be simulated digitally. The metal mining industry benefits from increased efficiency and remote site visualization. DTs also improve biopharmaceutical processes by ensuring consistent production without operator attention. In critical infrastructure protection, DTs provide early warning systems and enhance decision-making and coordination through AI algorithms. Gartner predicts that by 2027, over 40% of large companies will use DTs to increase revenue. The DT market, valued at \$8 billion in 2022, is expected to grow at a 25% CAGR from 2023 to 2032. Key industries include automotive, transportation, infrastructure, healthcare, energy, and aerospace.

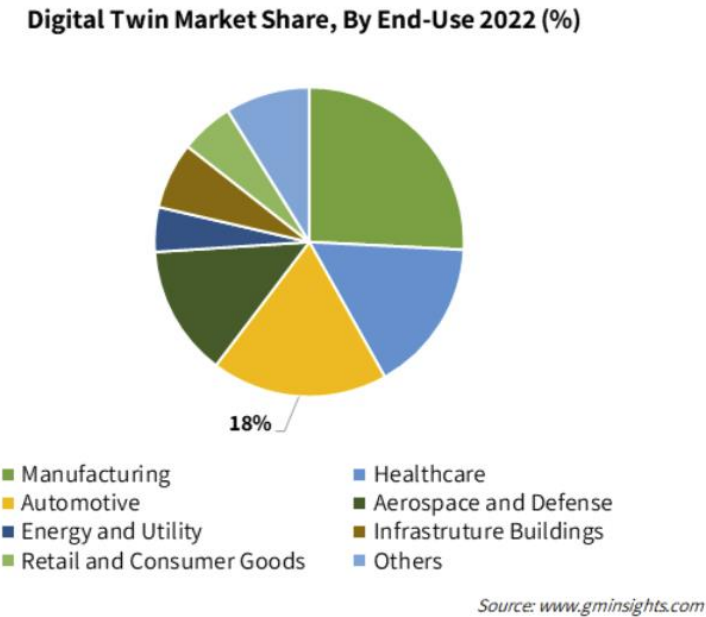


Figure 13. Digital Twin Market Share, By End-Use 2022 (%).

Digital Twins (DTs) are primarily used in engineering and manufacturing to create accurate virtual representations and simulate operational processes. NASA employs DTs for developing next-generation vehicles and aircraft. DTs are also applied in operations and supply chain management for traceability, transport maintenance, remote assistance, asset visualization, and design customization. Promising applications extend to various industries, including automotive, aerospace, construction, agriculture, mining, utilities, retail, healthcare, military, natural resources, and public safety. The industries using DTs can be seen in the following figure:



Figure 14. Industries using DTs.

The figure below highlights the impact of Digital Twins solutions in the business world.

Manufacturing	Aerospace/Automotive	Construction/Real Estate	Utilities
<ul style="list-style-type: none"> - Design customization - Simulate & validate each step of development - Enhancing Operations Process - Reducing overall cost of engineering - predictive maintenance - Virtually Monitor and manage performance 	<ul style="list-style-type: none"> - Design customization - Defect detection - Aircraft tracking - Stipulation of weather conditions - Optimizing the transport load - Vehicle defect detection - real-time monitoring and predictive analytics 	<ul style="list-style-type: none"> - Automated Project Control - Safety monitoring - Project Planning & Logistics - Building Performance Assessment - Evaluate space capacity and smartly design it - Quality assessment 	<ul style="list-style-type: none"> - Power grid planning - Enhanced visibility across physical grid - Efficiency improvement of the grid - Power grid self evaluation - Ecological reconstruction of the grid
Agriculture/Farming	Healthcare	Retail	Mining
<ul style="list-style-type: none"> - Advance smart farming - Plan, monitor, control, analyze & optimize farm processes - Weather prediction - Stress identification - Livestock monitoring & management 	<ul style="list-style-type: none"> - Diagnosis & therapy - Preventive treatment - Drug development - Medical device utilization - Facility & operations design - Education & training 	<ul style="list-style-type: none"> - Supply chain optimization - Product inception, development & distribution - Fleet management & route efficiency - Facility & operations design 	<ul style="list-style-type: none"> - Improve machinery productivity - Allow for realistic simulation training - Drug development - Medical device utilization - Facility & operations design - Education & training

Figure 15. Impact of Digital Twins solutions in the business world.

In the future, Digital Twins (DTs) could enable virtual walk-throughs of physical environments or products, improving prototyping and test simulations. New product categories can express brand identity in digital

form. DTs are expected to integrate with technologies like speech capabilities, augmented reality (AR), IoT, and AI.

Various sectors, including government agencies, infrastructure operators, technology companies, and research institutions, are investing in predictive analytics, DTs, and advanced monitoring for critical infrastructure. Government bodies regulate technology adoption and cybersecurity, while major industrial players in utilities, oil and gas, transportation, and telecommunications develop these technologies to enhance reliability and safety. Collaborations between public and private entities highlight the importance of advanced technologies in protecting essential services.

Despite this, as of 2022, 47% of IT decision-makers were unaware of DTs. In the future, DTs will expand to more use cases and industries, combining with AR for immersive experiences and AI for better insights and analytics. This will lead to even more applications of DT solutions in complex operations.

CSIM platform

Cyber and physical threats have increased due to technological advances, climate crisis, geopolitical instability, and terrorism. The adoption of Converged Security Information Management (CSIM) technology is driven by the need for comprehensive security solutions, centralized management, enhanced situational awareness, operational efficiency, regulatory compliance, integration with emerging technologies, and cost-effectiveness.

Industries benefiting from CSIM include critical infrastructure, emergency response services, private security, and public authorities. The CSIM market is growing due to increasing security threats, modernization of military and civil protection infrastructure, and demand for integrated awareness solutions.

CSIM integrates cybersecurity and physical security systems, enhancing overall security. It connects and manages security devices and software through a single interface, automating incident management. Current uses include unified security operations, real-time incident response, streamlined workflow, data correlation, and improved situational awareness. Future uses involve integrating AI, machine learning, IoT, and edge computing, enhancing predictive analytics, expanding IoT security management, facilitating cross-industry collaboration, and ensuring compliance with evolving regulations.

AI-based intrusion detection system (SigmoidS)

The rise of novel cyber threats has highlighted the need for timely network intrusion detection. The T4i DOVER® (upgraded) chemical detection technology is increasingly recognized for its importance due to environmental, industrial, and security concerns. It offers real-time monitoring, early detection of hazardous substances, and improved risk management. Advancements in sensor and UAV technology have made these systems more cost-effective and accessible, benefiting industries like infrastructure inspection, agriculture, oil and gas, environmental monitoring, military, and public safety.

The market for UAV-integrated chemical detection technology is growing rapidly, driven by industry demand, technological advancements, and regulatory requirements. A 20% growth in demand is expected over the next three years, with potential for higher growth due to emerging threats. Current uses of T4i

DOVER® on UAVs include environmental monitoring, industrial safety, defence, and emergency response. Major actors in defence, security, and environmental sectors are developing and using these technologies, with a trend towards UAV and UGV deployment for chemical detection.

T4i FemtoMachine®

Vapor generators are essential for calibrating analytical instruments in labs and field operations, especially for chemical detectors like the T4i DOVER. The T4i FemtoMachine® offers enhanced efficiency and reliability. Key industries benefiting from this technology include environmental sensors, refineries, critical infrastructures, military, and first responders.

The market for portable vapor generators is expanding due to technological advancements and regulatory requirements in sectors like pharmaceuticals and environmental monitoring. Current uses of the T4i FemtoMachine® include instrument calibration, generating precise vapor concentrations, and realistic training. Future uses may involve further miniaturization, IoT integration, and expansion into new industries.

Major actors in various sectors, including government agencies, companies, and industrial organizations, are involved in the development, regulation, and adoption of this technology. Geopolitical factors and regulatory changes also influence its development and adoption.

Activity Recognition and Explainable AI

The adoption of action recognition and explainable AI for critical infrastructure enhances security, safety compliance, preventive maintenance, operational efficiency, emergency response, and data analytics through real-time monitoring and analysis of behaviours.

Industries like security, manufacturing, healthcare, and retail benefit significantly, optimizing operations and improving safety and efficiency. The market for these technologies is growing rapidly, with action recognition being adopted in healthcare, retail, and automotive sectors, and explainable AI gaining importance for transparency and accountability.

Current uses include healthcare monitoring, fitness tracking, smart home automation, security, and driver assistance systems. Future applications could involve personalized healthcare, urban planning, workplace safety, customer experience, and human-robot collaboration. Additionally, ethical AI development, education, public policy, environmental monitoring, and criminal justice reform could benefit from explainability techniques to address biases and promote fairness. Major actors are involved in developing and regulating these technologies.

Autonomous resource allocation algorithms

Traditional resource allocation methods are often manual, inefficient, and error-prone. Autonomous algorithms analyse data in real-time, identify threats, and dynamically allocate resources to address risks quickly. This technology enhances security, operational efficiency, and resilience of critical infrastructures, allowing security personnel to focus on strategic tasks.

Industries benefiting the most include energy, transportation, telecommunications, and water infrastructure. Current uses of autonomous resource allocation include supply chain management, traffic management, security monitoring, emergency response, and infrastructure maintenance. Future uses could involve autonomous transportation, environmental monitoring, agriculture, public safety, and urban air mobility.

Significant interest and investment come from major economic, financial, industrial, and geopolitical actors. Defence contractors like Lockheed Martin, Northrop Grumman, and Boeing are developing autonomous drones for military applications, equipped with advanced resource allocation algorithms.

Diverse low-power hardware architectures for edge AI image processing based on Nvidia (GPU), IMX (NPU), Xilinx-FPGA (DPU)

Edge computing processes data locally instead of sending it to centralized cloud data centres, reducing latency and data transport costs. This is crucial for real-time data analysis in IoT devices and AI applications. The growth of 5G technology further drives the need for edge computing, benefiting industries like autonomous vehicles, manufacturing, smart cities, and healthcare.

The edge computing market, valued at \$3.6 billion in 2020, is expected to grow to \$15.7 billion by 2025, with a CAGR of 34.1%. Current uses include real-time analytics, IoT data processing, autonomous vehicles, and AI applications. Future uses may involve advanced AI/ML applications, enhanced IoT integration, and increased adoption in healthcare and manufacturing. Major companies like Nvidia and Lenovo are developing edge computing solutions, while governments and regulatory bodies focus on security and data privacy challenges.

HASP

The shift towards HASP technology aims to protect against cyber threats targeting the human element. HASP frameworks, like those developed by Picnic, align with industry standards and focus on social engineering risks. Benefits include improved security posture, reduced threats and operational expenses, lower attention fatigue at SOCs, and enhanced defence for high-value employees.

Industries benefiting from HASP technology include:

- Oil and Gas: Extended coverage, reliable connectivity, and quick deployment for remote operations.
- Telecommunications: High-speed connectivity and vast coverage with minimal infrastructure.
- Aerospace: Promoted by the HAPS Alliance for global harmonization and commercial adoption.

The global high altitude platforms market, valued at USD 1.54 billion in 2023, is expected to grow at a CAGR of 8.4% from 2024 to 2030. Current uses of HAPS include bridging the digital divide, rapid deployment in emergencies, enhanced mobile connectivity, and environmental sustainability.

Future Uses of HAPS Technology

The future of HAPS technology is promising, with significant advancements expected:

- **Industry Growth:** The global HAPS market is projected to exceed \$1 billion by 2025, driven by demand for enhanced connectivity. Major players like Airbus, Thales Group, and HAPS Mobile dominate the market.
- **Telecommunications:** Companies like Google and Facebook invest in HAPS to expand global internet access, revolutionizing communication networks.
- **Oil and Gas:** HAPS technology improves safety, optimizes operations, and ensures reliable data transmission, transforming oilfield communication.
- **Global Connectivity:** HAPS bridge communication gaps in remote areas, enhance disaster management, and improve remote sensing applications.

Major actors, including Airbus, Thales Group, and HAPSMobile, lead HAPS development. Regulatory bodies like EASA and FAA are establishing guidelines for safe deployment. HAPS technology is set to revolutionize industries by enhancing connectivity, promoting sustainability, and driving global integration.

Annex 4 – Competitive landscape

Three-dimensional representations of geometric data

- Competition intensity

3D mapping technology has several rivals in the market, who mainly provide solutions based on laser scanning, photogrammetry and GIS software. However, 3D mapping leveraging AI techniques is a topic that has recently garnered attention and therefore the competition is low/moderated.

The type of buyers can vary depending on the specific application required. Buyers may include private and public CI operators, engineering firms, construction companies, urban planning departments, emergency response organisations. Additionally, the size of the map can range from small-scale projects requiring limited coverage to large-scale ones involving extensive mapping of entire cities or regions. The cost for buyers to switch from one provider of 3D mapping technology to another can depend on several factors, including the level of integration with existing workflows and systems, the availability of compatible data formats, and the cost of retraining staff.

To enter the 3D mapping market, especially the AI-based, is challenging since it includes technological complexity and requires advanced expertise in AI, computer vision, image processing, spatial analytics, and software development. Moreover, the availability of high-quality data and how they will be obtained pose an additional challenge for new entrants.

There are various techniques for 3D mapping and modelling, including photogrammetry, LiDAR scanning, and Time-of-Flight (TOF) imaging. However, AI-based 3D mapping of large areas from 2D images is a topic that has not been extensively investigated. It is still at a research level, and the market for it is relatively small.

Overall, the limitations faced by CERTH in comparison to other competitors include the fact that CERTH is a research centre and not an industrial company with a specific product for specific needs. This means that CERTH exploits highly educated employees to provide customized solutions for every need and always at a state-of-the-art level.

- Competitors

Competitor: Pix4D

Competitor Description (Nationality, main activities, turnover, main customers): Pix4D is a market leader in photogrammetry software technology, providing mapping and 3D modelling solutions and data capture applications for various sectors including architecture and construction, agriculture, utilities and infrastructure, and public safety. Pix4D provides photogrammetry software for professional drone mapping.

Competitor solution comparison: Pix4D main customers include Architecture, Engineering & Construction, Agriculture, Energy, Utilities & Infrastructure and Forensics and Public safety. There may be potential overlap in customer segments, with our solution mainly focusing on critical infrastructure needs.

Pix4D solution is based on photogrammetry, a technique of taking multiple overlapping photographs and deriving measurements from them to create 3D models. A typical limitation in photogrammetry is that it is very challenging to produce reliable matches in regions with repetitive patterns, homogeneous appearance, or large illumination changes. Our solution investigates a more novel approach based on AI techniques to handle these limitations.

While Pix4D excels in 3D mapping and modelling from aerial data with photogrammetry, a mathematical technique, our solution focuses on the integration of AI models for the 3D reconstruction. Our goal is to build a model capable of precisely mapping environments with challenging conditions such as high altitudes, textures, weather conditions, etc.

Given that CERTH's solution follows a more research-oriented approach, conducting a direct comparison with Axis' product in terms of price, branding, and market experience is not feasible. However, in terms of innovation and value, CERTH's solution incorporates novel state-of-the-art algorithms and methods in the field, mainly AI-based to develop an algorithm with high performance in challenging environments, working at different altitudes, and with varying overlap percentages.

Thermal detector and localizer

- Competition intensity

Competition among research institutes and specialized firms in this market may be moderate. Institutes and companies continuously strive to develop more accurate, efficient, and cost-effective detection modules. However, since the market is relatively specialized and segmented, direct head-to-head competition may be limited to certain regions or specific applications. Collaboration and partnerships between institutes may also exist alongside competition, especially in advancing technology or addressing common challenges.

Suppliers of specialized components such as thermal/IR cameras and multispectral sensors may hold some bargaining power due to the specialized nature of these components. However, since there are multiple suppliers in the market, the power is somewhat mitigated. Research institutes may also have the capability to develop certain components in-house, reducing dependence on external suppliers. Also, the cost of switching technology and the potential for customization might mitigate this power to some extent.

Buyers could include government agencies, security firms, and other research institutions, and they may have moderate bargaining power. They typically search for cost-effective solutions without compromising quality and performance. However, since the demand for reliable surveillance solutions is relatively high, buyers may have limited alternatives, especially if the module offers unique features or superior performance that can be found in few alternatives.

Other research institutes might potentially develop similar detection modules. However, entry barriers could be moderate to high due to the need for expertise in AI, thermal imaging, and multispectral analysis. Intellectual property rights, patents, and proprietary technology could also act as barriers to entry, depending on your institute's capabilities. Further, establishing credibility, expertise, and gaining market share could be challenging.

While there may not be direct substitutes for multispectral detection modules based on thermal/IR cameras, alternative surveillance technologies and methods exist. For instance, traditional visual cameras, radar systems, sonar systems, LIDAR (Light Detection and Ranging) or satellite imagery may serve as partial substitutes in certain scenarios. However, these alternatives may not offer the same level of effectiveness under low-visibility conditions, fit for surveillance applications or provide multispectral analysis capabilities.

Overall, the limitations faced by CERTH in comparison to other competitors include the fact that CERTH is a research centre and not an industrial company with a specific product for specific needs. This means that CERTH exploits highly educated employees to provide customized solutions for every need and always at a state-of-the-art level.

The competitive advantages of CERTH and especially MKLab/M4D research group versus competition include the fact that they both have immense experience in security projects, specifically in those, which use multispectral detection and analysis technologies in UAV platforms. Since 2017 M4D group has participated and are still currently working on more than 10 projects, including CALLISTO, ROBORDER, ISOLA, 7SHIELD that exploited such technologies for surveillance purposes. This provides an advantage as the group is constantly improving and upgrading their existing techniques while at the same time it keeps track of the market trends of the relevant industry.

- Competitors

Competitor 1: InfraTec GmbH Infrarotsensorik und Messtechnik

Competitor Technology: Thermography Software IRBIS® 3

Competitor Description (Nationality, main activities, turnover, main customers): It is a control and analysis software for efficient measurement data acquisition and analysis as well as the creation of descriptive thermographic evaluations.

Competitor solution: "Thermography Software IRBIS® 3" appears to be specialized software designed for thermographic imaging and analysis. It likely facilitates the processing and interpretation of data from thermal cameras, primarily focusing on temperature measurement and analysis.

Our detection module focuses on providing surveillance capabilities using thermal/IR cameras to maximize detection during night and low-visibility weather conditions. It integrates thermal cameras with AI-based models for object identification and operates 24/7 under diverse weather conditions.

Competitor solution comparison: "Thermography Software IRBIS® 3" is more narrowly focused on thermographic applications, possibly used in industries like building inspection, electrical diagnostics, or industrial monitoring where temperature variations are critical. They focus on professionals and industries involved in thermography, such as building inspectors, maintenance technicians, and researchers. Our module has a broader scope, with a focus on surveillance applications and offering multispectral analysis capabilities. It targets scenarios where visual cameras may be ineffective due to low visibility. The interested industries may include security, defence, and infrastructure monitoring.

Thermography Software IRBIS® 3 may have limitations compared to the multispectral detection module, particularly in terms of surveillance capabilities, AI integration, and market targeting. It may lack the real-time surveillance capabilities and object identification features offered by our module. It also may not feature advanced AI capabilities for object identification and classification. Further, it primarily targets industries and professionals involved in thermography applications, such as building inspection and maintenance, while our module targets surveillance applications across various industries, including security, defence, and infrastructure monitoring, offering broader market appeal.

While Thermography Software IRBIS® 3 excels in thermographic imaging and analysis, particularly in temperature measurement and analysis for various industrial applications, our solution offers a broader scope of functionality tailored specifically for surveillance purposes. Our module integrates thermal/IR cameras with AI-based object identification and multispectral analysis, enabling real-time detection and classification of objects or threats in low-visibility conditions. Additionally, our solution provides 24/7 surveillance capabilities across diverse environmental conditions, offering enhanced versatility and adaptability for security, defence, and infrastructure monitoring applications.

Our multispectral detection module surpasses Thermography Software IRBIS® 3 in several key aspects. With advanced surveillance capabilities, including real-time object detection and classification in low-visibility conditions, our module offers a comprehensive solution beyond the primary focus of temperature measurement in thermographic imaging. The research institute's strong track record in innovation and research, coupled with extensive EU project implementation experience, establishes it as a trusted partner in the surveillance technology landscape. The module's scalability further enhances its value proposition, positioning it as a reliable and forward-thinking choice for organizations with diverse security needs.

Competitor 2: CC-KING

Competitor Technology: Object detection using data fusion from multispectral camera sensors.

Competitor Description (Nationality, main activities, turnover, main customers): This multispectral detection module exploits data from thermal/IR cameras and employs AI-based models for object identification and analysis. In contrast, the KI Engineering solution focuses on data fusion from multispectral camera sensors, likely combining information from different spectral bands for improved object detection and classification. Both solutions aim to enhance object detection capabilities using specialized sensors nonetheless different approaches are adopted.

Our solution: Streams from thermal cameras will be fed to the AI-based model in order to identify objects of interests/threats. The outcomes of the analysis are provided to the system for further assessment.

Their solution: The solution proposed from KI Engineering mostly targets to improve the detection accuracy by pre-processing the two streams producing one single scene representation as it is depicted in the below schema. As such, it is considered that a potential detector could perform more robust.

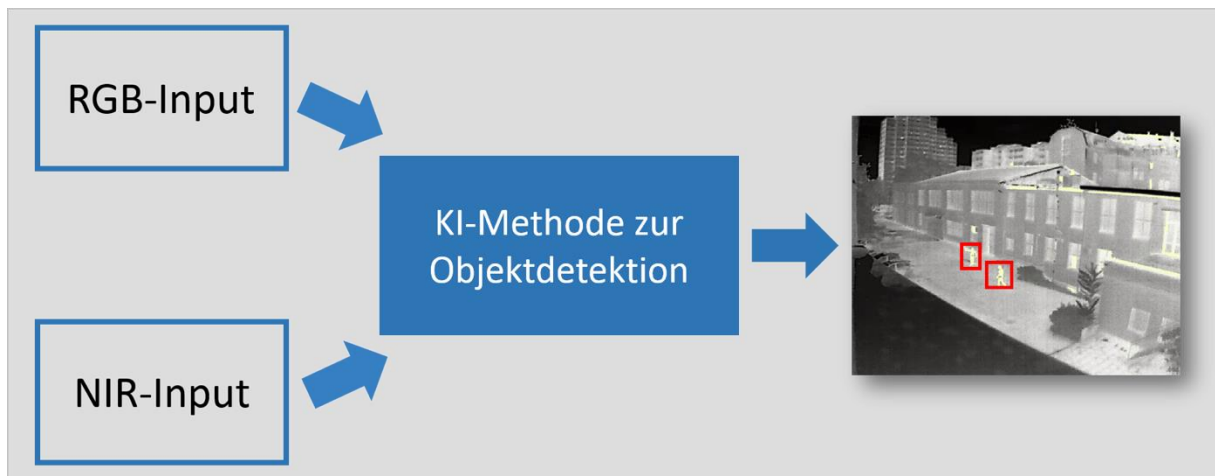


Figure 16. KI Engineering Solution.

Competitor solution comparison: CC-KING is the competence centre for AI Systems Engineering of the Karlsruhe research institutes Fraunhofer Institute of Optronics, Systems Engineering and Image Exploitation IOSB, FZI Research Centre for Information Technology and Karlsruhe Institute of Technology (KIT). It connects top-level AI research and established engineering disciplines and thus aims to facilitate the practical application of methods of AI and ML.

While there may be potential overlap in customer segments between our multispectral detection module and the KI Engineering solution, their research areas are focused on Automated mobility and other future topics that require robust environment perception. Among other things, camera-based systems are used for this purpose. A central and safety-critical challenge is the reliable perception of vulnerable road users (VRUs), such as vehicles or cyclists, regardless of the prevailing visibility and lighting conditions.

On the other hand, our research within TESTUDO is a module that will deliver a 24/7 detection service and ensure operations under diverse weather condition that affects the capacities of visual cameras for surveillance purposes.

Their solution is based on the fusion of complementary image information from the visible light spectrum and the near infrared spectrum (NIR). While a conventional camera will perform to its full detection potential in good visibility conditions, an infrared camera can significantly improve robustness in difficult visibility conditions, especially in darkness, fog, or rain. Our solution provides ML/DL detection models for processing thermal/IR streams and produce Bounding Box at the projection plane (position of objects of interest and detection confidence score). Hence, both approaches display the same objective (object detection) though different schemas are adopted.

The accuracy of object detection may vary between the two solutions based on factors such as sensor technology, data processing algorithms, and environmental conditions. Both solutions likely require integration with existing surveillance or monitoring systems.

The testing of the developed AI method by CC-KING can take place within the framework of the Test Area Autonomous Driving Baden Württemberg (TAF-BW) from a large-scale infrastructure perspective, or with the help of the automated test vehicle CoCar from the FZI vehicle fleet.

Our multispectral detection module offers advanced surveillance capabilities with real-time object detection and classification using thermal/IR cameras, providing reliable performance in low-visibility conditions. While the KI Engineering solution employs data fusion from multispectral camera sensors for object detection, the specifics of its surveillance capabilities and effectiveness in challenging environments may vary.

The KI Engineering solution appears to have a broader application scope, potentially catering to various industries beyond surveillance, such as mobility, transportation, and industrial automation.

Their existing solutions include: Testing Imaging Transition of Information (I-TO-I) between connected vehicles, Data acquisition for object detection from vehicle perspective, RISC-V development environment for TensorFlow Lite models, Traffic light detection, Obstacle and Object Recognition for Mobile Robots using AI.

Our research focus is developing intelligent frameworks for combining, fusing (at different levels) and interpreting observations from a number of different sensors and/or multimedia to provide a robust and complete description of an environment, behaviour or process of interest, as well as decision support, analytics and retrieval applications.

Automatic object detection and identification from visual spectrum

- **Competition Intensity**

Visual object detection is a highly researched task, with institutes and companies continually striving to develop more accurate, efficient, and cost-effective detection modules. However, competition in the surveillance field is moderated due to the specialised and segmented nature of the market.

Buyers could range from large enterprises or government agencies with substantial budgets and significant orders to smaller businesses or organisations with more modest budgets and requirements. Both categories are seeking highly performant and cost-effective solutions that will meet their specific needs. The cost for a buyer to switch to another competitor necessitates the construction of a new tailor-made solution based on the buyer's specific needs, which is time and resource consuming.

Entering the real-world visual object detection market can be challenging due to the required technological expertise (machine learning, computer vision), the availability of real-world data for training AI models (collection, annotation), the necessary hardware resources, and the competition with established players. However, there is space for new innovative solutions that address specific needs.

A robust, highly performative object detection solution tailored to the buyer's specific needs and real-world environments requires specialized expertise and resources, large, diverse, and well-labelled datasets, as well as high-performance hardware and specialized infrastructure. Therefore, the ease of substitution depends on these factors and the competitor's ability to address them.

- **Competitor**

Competitor: Axis Communications

Competitor Technology: Axis Communications AB is a Swedish manufacturer of network cameras for the physical security and video surveillance industries. It is a provider of IP-based video surveillance solutions, offering a range of network cameras, video encoders, video management software, and accessories.

Competitor Description (Nationality, main activities, turnover, main customers): Axis Communications provides an AI-based object detection and classification solution that comes preinstalled on Axis network cameras, capable of detecting and identifying humans, vehicles, or types of vehicles including cars, trucks, buses, and bikes.

Competitor Solution comparison:

Axis Communications' main customers include businesses, government agencies, and organisations that require surveillance, security, and monitoring systems. Therefore, there is potential overlap in customer segments, with our solution mainly focusing on critical infrastructure protection and needs.

The main limitation of the Axis solution compared to ours is that it provides predefined object categories (human, vehicle) for detection and is not customizable to each buyer's different needs, which may include other types of objects for detection. Additionally, the Axis solution is camera-dependent and is only provided in combination with Axis network cameras and the Axis camera management system.

Given that CERTH's solution follows a more research-oriented approach, conducting a direct comparison with Axis' product in terms of price, branding, and market experience is not feasible. However, in terms of innovation and value, our solution incorporates state-of-the-art algorithms and methods in the field, allowing buyers to create a customizable tool with various object categories, beyond humans and vehicles, depending on their needs. Furthermore, our software is camera-independent and compatible with different cameras across brands and specifications.

Event Predictor

- Competition Intensity

Research institutes in Europe and around the world are likely to be active in developing similar modules. The intensity of competition will depend on the number of institutes working in the same field, their expertise, resources, innovative approaches and the quality of their predictive models and decision-making frameworks. The competition may be high with other entities working on similar projects with comparable capabilities.

In the context of research institutes, supplier power may not be as relevant as in industries like manufacturing or retail. However, depending on the availability and cost of certain technologies (such as XR technologies, EvoNET, Neural Networks), there might be a moderate level of supplier influence. The power of suppliers would depend on the availability of alternative sources and the uniqueness of the resources they provide.

In this context, the buyers could be funding agencies, government organizations, private companies, or other research institutes looking to collaborate or obtain technologies that implement predictive analysis and decision-making frameworks in their operations. If there are many potential buyers for such

technologies, they may have significant power in negotiating prices and terms. However, our module offers unique features based on the specialized knowledge of the institute specifically for surveillance operations and can address specific needs not met by other solutions. Additionally, the buyer power may vary depending on the specific project requirements, budget constraints, and the availability of alternative solutions in the market.

Established research institutes and organizations with expertise in data analytics, machine learning, and decision science may pose a significant threat if they decide to enter the market or participate in similar projects. New players or collaborative efforts could emerge, especially from academia or startups. However, barriers to entry such as the need for specialized knowledge, access to data, established networks and research capabilities may limit the entry of new competitors.

The specific combination of Evolutionary state graph network (EvoNET), Neural Networks, and Cox Regression for event prediction, along with 3D representation schemas and XR technologies, creates a unique proposition. However, substituting such a specialized module with an equivalent alternative might be challenging. Additionally, advancements in the field of predictive analytics, decision-making frameworks, and digital twin technology could lead to the emergence of new substitutes over time.

Overall, the limitations faced by CERTH in comparison to other competitors include the fact that CERTH is a research centre and not an industrial company with a specific product for specific needs. This means that CERTH exploits highly educated employees to provide customized solutions for every need and always at a state-of-the-art level.

The competitive advantages of CERTH and especially MKLab/M4D research group versus competition include the fact that they both have immense experience in security projects, specifically in those, which use modules for event prediction. This provides an advantage as the group is constantly improving and upgrading their existing techniques while at the same time it keeps track of the market trends of the relevant industry.

Data Collection from UAV and process to the edge

- **Competition Intensity**

The European drones market is highly fragmented, with several players accounting for significant shares in the market. Some of the prominent companies in the European drones market are Azure Drones SAS, Parrot Drones, Terra Drone, Onyx Scan Advanced LiDAR Systems, and AltiGator Unmanned Solutions. The companies are spending heavily on improving technology and introducing new features in drones to support various commercial applications. For instance, in September 2019, Parrot Drones introduced a drone with a smartphone-powered first-person view.

The camera is powered with a 4K HDR 21 megapixel sensor and comes with long-lasting battery life, which can be used for shooting advertisements and other entertainment applications.

The launch of such advanced drones for various applications is anticipated to help companies expand their presence in the region. Furthermore, with the ease in drone regulations, many companies are entering the drones industry of Europe, which is expected to further increase the competition among the players in the future.

- Competitors

Competitor 1: ELISTAIR

Competitor Technology: ORION 2 Tethered UAV - Advanced Tethered UAV for military and public order agencies

Competitor Description (Nationality, main activities, turnover, main customers): USA – EU (FRA), tethered UAV manufacturers.

Main customers include private and public security organisations.

Elistair designs and manufactures tethered drone systems, offering extended flight times, increased safety and secured high-speed data transfer, for persistent surveillance and communications. The company's products are deployed by police forces, public safety departments, private security companies and government in over 30 countries. Elistair has received up to 9.5M EUR in funding (Grant, Seed, Series A & B) at the time of this Report to further develop its technology offering.

Competitor solution: ORION 2 is capable of operating for 24 hours continuously at 100 meters (330 feet) height with 2 kg of payload and extended detection ranges up to 10 kilometres. Gimbal stabilization and crystal-clear imagery with low latencies. Optical Zoom x30 - EO Channel Specs 1080p Full HD - IR Channel Specs 640x480 - IR Digital Zoom x4. Automated Deployment, Smart Parachute, Secure Data Link – transfer speed up to 200 mb/s. Weather-resistant with an IP54 rating. Mission Operation Software “T-Planner”: digital stabilization, a map overlay of the drone's location and camera POV. EO and IR images are streamed simultaneously. IP based video stream allows external sharing of the video feeds such as streaming, processing, integration into third party software and VMS.

Competitor solution comparison:

Technical Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Algorithm/Software Source	“T-Planner”: competitor's own software
2	GPU AI Decision Support	Detect and track capabilities
3	UAV Neutralization/automation	Yes. Automatic take-off / landing, altitude
4	Image / Video Processing, Threat Detection and Forecasting	Image / Video Processing, Yes. Threat Detection and Forecasting, No.
Functional Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Human detection	Yes. Detect and track.
2	Object detection	Yes. Detect and track.
Commercial criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	User friendly	Yes. Operation Setup in minutes. Single operator, Automated take-off, climb and land procedures.
2	Ecosystem friendly	Modular, hot-swappable arms/legs
3	Continued technical support and updates	Dependent on Competitor software update frequency

Competitor 2: DronesLab B.V. VERTICAL Technologies

Competitor Description (Nationality, main activities, turnover, main customers): DronesLab B.V. VERTICAL Technologies is a UAV manufacturer, specialised in long-range Mapping and Surveillance UAVs. Based in Badhoevedorp, Netherlands ANNUAL REVENUE 2018 USD \$1.87 Million.

Competitor solution: Fully autonomous from take-off to landing. Automatic object tracking & object following. Simple manual control using the DeltaQuad Controller. Tool-less 1 minute field assembly. No pre-flight calibrations are required. Covering up to 100KM / 150KM in a single flight. Redundant flight system. Online mission validation & log analysis tools. Automatic object following. DeltaQuad Pro #VIEW with surveillance package 3 can automatically follow a moving object. Proprietary control software allows the system to safely and intelligently follow a human, car, vessel, or even another UAV. Transmission range of up to 50KM, HD quality video from a hand-held remote controller. Unlimited range by streaming both HD video and UAV control over a VPN secured mobile connection (4G, 5G).

Surveillance package 3: Dual Thermal (IR) and RGB (EO) controllable turret gimbal Industrial-grade thermal & RGB (EO/IR) surveillance package, Nighthawk2-V computer-controlled retractable gimbal. 360-degree control, 40x zoom. Stabilization, automatic object tracking and object following by touchscreen tapping on an object, and HD recording. The camera is controlled using the DeltaQuad Controller or from an additional Camera Control Laptop. Instant switching between RGB and Thermal vision. Thermal & RGB live video Pan, Tilt & 40x zoom control, Touch screen object tracking & stabilization, Automatic object following, Target coordinates & altitude, GPS controlled camera position holding, Onboard recording.

Competitor solution comparison:

Technical Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Algorithm/Software Source	Competitor Proprietary Software
2	GPU AI Decision Support	Detect, track, follow capabilities. Identify and distinguish human, car, boat, other UAV
3	UAV Neutralization/automation	Tool-less operation set up. Minimized setup time. Airborne in 2 minutes. Automatic take-off/landing
4	Image / Video Processing, Threat Detection and Forecasting	Image / Video Processing, Yes.
Functional Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Human detection	Yes. Detect, track and follow autonomously.
2	Object detection	Yes. Detect, track and follow autonomously.
Commercial Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	User friendly	Medium. Single operator, continuous monitoring, Automated take-off/landing.
2	Ecosystem friendly	
3	Continued technical support and updates	Dependent on Competitor software update frequency

Competitor 3: HEIGHT TECHNOLOGIES

Competitor Technology: G3 Tactical Drone VTOL

Competitor Description (Nationality, main activities, turnover, main customers): HEIGHT TECHNOLOGIES manufactures technologically highly developed drones equipped with cameras, sensors and measurement equipment, in Meerbusch, Nordrhein-Westfalen, Germany. Military and Security oriented UAVs. Geldermalsen, The Netherlands.

Competitor solution: Simple, compact, lightweight & modular design Ruggedized, dust and rain proof 1 man required for rapid deployment and operation Designed for ISTAR missions. The G3 is equipped with a gimbaled, stabilized high-performance EO & IR camera. Payloads are interchangeable with other sensors such as communication jammers, electronic warfare etc. can be configured to hold any kind of sensor up to 3 kg. Transportable with a standard Jeep and designed for longer, more complicated missions. Less than 5-minute assembly, swappable batteries, and sensors. Up to 90 minutes flight time, 5km range, 30-300m AGL, -10 to +50 C operating temperature, Data uplink, telemetry, and video downlink, day & night real-time HQ video.

Competitor solution comparison:

Technical Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Algorithm/Software Source	Competitor Proprietary Software
2	GPU AI Decision Support	Up to 3kg sensor, no built-in detect & tracking
3	UAV Neutralization/automation	Automated take-off/landing. Simple controls.
4	Image / Video Processing, Threat Detection and Forecasting	EO/IR camera system up to 3kg. No AI Threat Detection and Forecasting.
Functional Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Human detection	Not built-in
2	Object detection	Not built-in
Commercial Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	User friendly	5-minute setup. Easy manual /control
2	Ecosystem friendly	
3	Continued technical support and updates	Dependent on Competitor software update frequency

Competitor 4: HEIGHT TECHNOLOGIES

Competitor Technology: PD1 VTOL Unmanned Aerial System

Competitor Description (Nationality, main activities, turnover, main customers): HEIGHT TECHNOLOGIES manufactures technologically highly developed drones equipped with cameras, sensors and measurement equipment, in Meerbusch, Nordrhein-Westfalen, Germany. Military and Security oriented UAVs. Geldermalsen, The Netherlands.

Competitor solution: The PD1 is a hybrid-powered VTOL fixed-wing ready-to-fly solution UAV, standard equipped with an EO/IR camera system, encrypted LR data link and ground control station. 10+ hours

flight time, 3km service ceiling, 10kg payload, 100km live full HD video, 500+ km operational range. 4m wingspan, 2.5m length, 4-stroke propulsion with runway/catapult/VTOL take-off methods. PD-1 VTOL

CONVERSION KIT: fully automatic take-off and landing, can be operated on the ship, can hover for a limited time, less space for take-off/ landing. Target tracking, scene lock.

COAST GUARD AND MARITIME OPERATIONS Use PD-1 VTOL system for fast deployment and response time. Upgraded with movement detection system—specially adjusted for maritime operation—USG-212 gimbal allows you to automatically detect small targets, such as people in the water, fishing boats, jet skies and so on. The PD-1 VTOL conversion kit will allow you to operate the drone from the vessel for a rapid response while the command-and-control centre will give an advantage of a single environment for all your units to get real-time information on the go and to record all videos and events. Additionally, the package delivery system will allow you to drop a lifesaving buoy.

Competitor solution comparison:

Technical Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Algorithm/Software Source	Competitor Proprietary Software
2	GPU AI Decision Support	Detect, Track, Follow
3	UAV Neutralization/automation	VTOL autonomous take-off & landing with VTOL KIT, pre-programmed autonomous flight path
4	Image / Video Processing, Threat Detection and Forecasting	Night/Day live stream full HD video. No built in threat Detection and Forecasting
Functional Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	Human detection	Yes. Can detect humans in water, on boats, land, etc
2	Object detection	Yes. Can detect small boats, jet skis, etc.
Commercial Criteria		
	Technical Comparison Criteria	Competitor Solutions Performances
1	User friendly	Medium. Autonomous take-off/landing easy use controller
2	Ecosystem friendly	
3	Continued technical support and updates	Dependent on Competitor software update frequency

AI-based intrusion detection system (SigmoIDS)

- Competition Intensity

As the network cybersecurity market rapidly grows, many leading IT firms are proposing tools for intrusion detection.

For AI-based IDS, the only entities that could be identified as “suppliers” are firms providing training datasets. However, in the case of SigmoIDS, the data used for training is produced by the local network.

Therefore, supplier power does not have an impact on SigmoIDS service.

Being deployable in any internal network, SigmoIDS is not bound to any specific clients. Nevertheless, its development should always take into account buyers’ needs, as for any other product.

Well-established firms may constitute an obstacle for the market entry. Other entry barriers may include free open-source network IDS, which, albeit possibly less effective, are often considered reputable and trustworthy.

Intrusion detection solutions are bound to remain relevant, as new cyber threats emerge rapidly.

- Competitors

Competitor 1: Palo Alto Networks

Competitor Technology: Intrusion detection and prevention system

Competitor Description: U.S. cybersecurity company providing next-generation firewalls, cloud and network security solutions.

While both this solution and SigmoidIDS are designed to be efficient AI-based intrusion detection systems. However, Palo Alto Network, like most commercially available IDS, relies on rule-based detection to identify threats. SigmoidIDS, on the other hand, utilizes an anomaly-based approach, which detects attacks by analysing unexpected changes in the network traffic.

Although the client base is similar, these two products offer complementary solutions.

Rule-based (or signature-based) approaches are limited by the need for rules to be general and be valid for any network. However, a state-of-the-art network IDS must take into account the regular traffic of a network to effectively identify malicious activity. Traffic that could be normal for one network may be indicative of an ongoing attack for another.

This company is currently a leader in the market. In terms of outreach and branding, it holds an undeniable advantage. Nevertheless, the actual accuracy of their product in detecting novel threats is unclear, at least according to the information that is publicly available.

SigmoidIDS has the potential to find anomalies in the traffic that may be overlooked by rule-based systems.

T4i DOVER® (upgraded)

- Competition Intensity

Competitive rivalry may be moderate to low, considering that T4i DOVER® technology offers unique features not available in competitors' products, such as GC-PID technology and the capability to sample from both air and water. However, there may still be competition from companies offering alternative chemical detection solutions, albeit with different technology platforms.

Supplier power may vary depending on the availability of components specific to GC-PID technology and generally the technology that responds to T4i DOVER®.

Buyer power could be moderate to high, as buyers may have preferences for specific detection technologies or features based on their requirements. However, the unique capabilities of GC-PID technology and the ability to sample from water could give our company some negotiating power with buyers seeking comprehensive detection solutions.

The threat of new entry varies based on barriers to adopting GC-PID technology. While the specialized nature and expertise required may discourage some potential entrants, technological advancements and regulatory factors could still attract new competitors. Monitoring the market closely is essential.

The threat of substitution may be reduced, as competitors offering PID or IMS technology may not fully replicate the capabilities of T4i DOVER® technology (GC-PID), especially regarding the ability to sample from water. However, alternative detection methods or technologies could still pose some level of substitution risk, particularly in specific applications or environments.

- Competitors

Competitor 1: FLIR

Competitor Technology: MUVE C360

Competitor Description: Both T4i DOVER® and FLIR MUVE C360 are designed for surveillance provide real-time continuous monitoring of chemical hazards while on the move.

Both T4i DOVER® and FLIR MUVE C360 addressed to emergency responders, industrial safety officers, and environmental monitoring experts.

This technology is designed to analyse vapours and not liquid samples. The competitor has no identification capabilities for hazard compounds and only provides alerts. T4i DOVER® in the framework of TESTUDO will include a liquid sampler to automatically collect the water sample.

FLIR MUVE C360 is a hand portable device easily to be mounted on UAVs and includes a photoionization detector (PID), Lower Explosive Limit (LEL) detector, and six other sensors, while T4i DOVER® provides identification together with quantitative analysis along with the coordinates that it was detected. T4i DOVER® is not a passive detector as competitor and withstands sudden changes of altitude, pressure & temperature. It is also using isokinetic sampling with a unique sample that allows valveless dynamic sampling.

T4i DOVER® incorporates a chemical separation step thanks to gas chromatography technology. This feature enhances the detection of compounds with greater effectiveness and accuracy. Furthermore, T4i DOVER® boasts unique sampling capabilities, a crucial asset particularly in scenarios where the detector may be exposed to high concentrations of potentially harmful chemicals.

Competitor 2: Bruker

Competitor technology: RAID M-100

Competitor solution: Both T4i DOVER® and Bruker RAID M-100 are able to detect and identify CWAs and TICs. However, has proven its capability to dynamically run detection & identification on UAVs.

Competitor description: Competitor's technology is designed to analyse vapours and not liquid samples. It is not designed to be integrated in UAVs like T4i DOVER® will include a liquid sampler to automatically collect the water sample.

Bruker RAID M-100 consist of an IMS detector while T4i DOVER® has a PID detector. Bruker is an established well-known company both in Europe and all over the world. Many of their instruments are of high quality and performance and are used by agencies and military teams. However, T4i DOVER® has filled in the gap in airborne chemical detectors in particularly UAVs.

T4i DOVER® incorporates a chemical separation step thanks to gas chromatography technology. This feature enhances the detection of compounds with greater effectiveness and accuracy. Furthermore, T4i DOVER® boasts unique sampling capabilities, a crucial asset particularly in scenarios where the detector may be exposed to high concentrations of potentially harmful chemicals.

Competitor 3: Environics

Competitor technology: ChemPro100i

Competitor solution: Both T4i DOVER® and Environics are able to detect and identify CWAs and TICs. T4i has exclusively designed as payload in UAVs. Environics has designed the ChemPro100i as a handheld and proposes it as a payload in UAVs.

Competitor description: This technology is designed to analyse vapours and not liquid samples. T4i DOVER® in the framework of TESTUDO will include a liquid sampler to automatically collect the water sample.

Environics ChemPro100i consists of an IMS detector while T4i DOVER® has a PID detector. Both technologies have a similar weight and they can be man portable. They both have low detection limits. However, IMS is famous for identification capability being very fast and with the limitation of quickly poisoning.

T4i DOVER® incorporates a chemical separation step thanks to gas chromatography technology. This feature enhances the detection of compounds with greater effectiveness and accuracy. Furthermore, T4i DOVER® boasts unique sampling capabilities, a crucial asset particularly in scenarios where the detector may be exposed to high concentrations of potentially harmful chemicals.

T4i FemtoMachine®

- Competition Intensity

The competitive rivalry may be moderate to low due to the absence of hand portable vapor generators in the market. Currently there is no competitive product for the field. However, competition could still arise from alternative calibration solutions or from competitors developing similar portable devices in the future.

Given the unique nature of hand-portable vapor generators, the bargaining power of suppliers for specialized components or technology specific to these devices may vary. Suppliers with exclusive access to essential components may have some leverage, but the overall impact could depend on the availability of alternatives and the extent of vertical integration within the industry.

Buyers seeking hand-portable vapor generators may have limited options due to the absence of direct competitors offering similar products. This could potentially reduce buyer power, as customers may be willing to pay a premium for the unique features and functionality provided by these devices.

Established companies may be hesitant to enter this market without a clear advantage or sufficient demand to justify investment.

While there may not be direct substitutes for hand-portable vapor generators, customers may consider alternative solutions for calibration or vapor generation, such as stationary equipment or manual methods. However, the unique portability and convenience offered by hand-portable vapor generators may mitigate the threat of substitution to some extent.

- Competitors

Competitor 1: Owlstone

Competitor technology: OVG-4

Competitor solution: Both T4i FemtoMachine® and Owlstone OVG-4 are used vapour generators but they do have different specifications.

The main and most important limitation is that T4i FemtoMachine® is a portable field vapour generator and can be used for both indoors and outdoors purposes, while the use of Owlstone OVG-4 is limited to be used as bench top device.

Available analytes, target compounds, are the same for both solutions. Owlstone OVG-4 can produce lower levels of chemical concentration than T4i FemtoMachine® but T4i FemtoMachine® has a wide range of flows that can be achieved. T4i FemtoMachine® does not use dangerous and costly gas cylinders for air supply rather than ambient air while Owlstone OVG-4 uses nitrogen.

T4i FemtoMachine® is more an economical solution and designed to be used outdoor and in field conditions expanding the market and increasing the potential customers.

Competitor 2: VICI Valco

Competitor technology: Dynacalibrator 120

Competitor solution: Both T4i FemtoMachine® and VICI Dynacalibrator 120 are used vapour generators but they do have different specifications.

The main and most important limitation is that T4i FemtoMachine® is a portable field vapour generator and can be used for both indoors and outdoors purposes, while the use of VICI Dynacalibrator 120 is limited to be used as bench top device. (It weighs 5 times more than T4i FemtoMachine®).

Available analytes, target compounds, are the same for both solutions. VICI Dynacalibrator 120 has a longer operation time than T4i FemtoMachine® but T4i FemtoMachine® is able to provide a wider range of concentrations.

T4i FemtoMachine® is designed to be used outdoor and in field conditions expanding the market and increasing the potential customers. It serves the needs for device calibration in the field.

Competitor 3: Hovacal

Competitor technology: HovaGas

Competitor solution: Both T4i FemtoMachine® and Hovacal HovaGas are used vapour generators but they do have different specifications.

The main and most important limitation is that T4i FemtoMachine® is a portable field vapour generator and can be used for both indoors and outdoors purposes, while the use of Hovacal HovaGas is limited to be used as bench top device. (It weighs 5 times more than T4i FemtoMachine®).

Available analytes, target compounds, are the same for both solutions. T4i FemtoMachine® can produce a wider range of concentrations than HovaGas is able to.

T4i FemtoMachine® is designed to be used outdoor and in field conditions expanding the market and increasing the potential customers. It serves the needs for device calibration in the field.

Activity Recognition and Explainable AI

- Competition Intensity

The competitive rivalry is moderated by the fact that technologies are transferred and tailored to the specific needs of the project, potentially mitigating direct head-to-head competition. Supplier power remains low, given the flexibility in technology sourcing. Conversely, buyer power is high due to the customization of solutions to suit specific use cases, leading to minimal competition in certain niches. However, the threat of new entrants is moderate, as the industry's specialized nature may pose barriers to entry, albeit not insurmountable. The constant development of substitute technologies heightens the threat of substitution, requiring continuous innovation and adaptation to maintain competitiveness.

- Competitors

The origin the solution makes it difficult to establish a direct competitor and as a non-profit research centre, VICOM doesn't establish itself against possible competitors.

Autonomous resource allocation algorithms

- Competition Intensity

In the realm of competitive rivalry, existing commercial solutions offer autonomous resource allocation, primarily with larger system for fleet/mission management systems but fall short of fulfilling all objectives of the TESTUDO project. Many such platforms include only aerial drones, typically drones from the same manufacturer. Moreover, most solutions necessitate the installation of specialized hardware, indicating a gap in fully comprehensive multi-modal autonomy. Supplier and buyer power are intertwined, with customized solutions imperative for integration with legacy systems, highlighting a reliance on specific providers. While the threat of new entrants is palpable given the evolving technology landscape and growing demand for multi-modal robotic solutions, the barrier to entry may be elevated due to the specialized nature of the industry.

- Competitors

Competitor 1: Auterion

Competitor solution: This solution is fully commercialized solution with user-friendly user interfaces, but seemingly lacks the ability to optimize coverage for several mobile sensor platforms, as a result is not the same with Autonomous resource allocation algorithms.

SINTEF is a research organization and has no commercial ambitions for the software algorithms at the present time.

A different point between Auterion and SINTEF's technology is that Auterion brings new value of providing the ability to optimize the use of several mobile assets.

Competitor 2: Skydio

Competitor solution is not the same with SINTEF because is tightly coupled with the drone hardware and is only available for Skydio drones.

The solution requires Skydio aerial drones and is not useable for other platforms. It is unclear if it will be able to optimize coverage given multiple drones.

A different point between Auterion and SINTEF's technology is that Auterion brings new value of providing the ability to optimize the use of several mobile assets.

Competitor 3: Clearpath Robotics

Competitor solution: It is fully commercialized solutions with user-friendly user interfaces, but seemingly lacks the ability to optimize coverage for several mobile sensor platforms.


The solution targets ground vehicles only and not aerial drones. Seemingly no built-in multi-vehicle optimization algorithms.

While Clearpath may excel in offering a mature solution with user-friendly interfaces, SINTEF's solution stands out with its advanced capability to optimize mission objectives across multiple mobile sensor platforms. Unlike Clearpath, brings a unique value proposition by providing the ability to optimize the utilization of various mobile assets, offering optimized paths for use cases involving both UAS and UGVs. This versatility allows SINTEF to cater to a broader range of scenarios and industries, enhancing efficiency and effectiveness in diverse operational environments. Moreover, SINTEF's commitment to innovation ensures that it continuously evolves its product offerings, staying ahead of the curve in delivering cutting-edge solutions to its customers.

Diverse low-power hardware architectures for edge AI image processing based on Nvidia (GPU), IMX (NPU), Xilinx-FPGA (DPU)

- Competition Intensity

In the landscape of non-profit research in embedded AI, competitive rivalry remains moderate, as companies focus on niche markets. Supplier power is low, given the availability of various suppliers for



embedded system components. However, buyer power is high, as the technology serves a specific market segment with unique requirements. The threat of new entry is also high, given the specialized nature of the market, while the threat of substitution looms large due to decreasing barriers to entry in AI and embedded systems. These dynamics underscore the need for continuous innovation and differentiation to maintain competitiveness in this evolving landscape.

- Competitors

As a non-profit research centre, TEKNIKER operates in a unique landscape where direct competition is minimal and primarily comes from other research institutions. Its core focus is on the generation and advancement of knowledge, rather than competing in a traditional commercial sense.

Annex 5 – Market Analysis Survey



TESTUDO

HORIZON-CL3-2022-INFRA-01- Grant Agreement No. 101121258

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES IN
INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

T11.3 Market analysis and potential business models

Market Analysis Survey

This survey is addressed to project partners only. Thank you for your input.

1. Which Consortium partner do you work for?

- | | | |
|----------------------------------|---------------------------------|----------------------------------|
| <input type="checkbox"/> ACCELI | <input type="checkbox"/> ENG | <input type="checkbox"/> TEK |
| <input type="checkbox"/> STWS | <input type="checkbox"/> PIAP | <input type="checkbox"/> DRAXIS |
| <input type="checkbox"/> NTTD IT | <input type="checkbox"/> T4i | <input type="checkbox"/> ADS |
| <input type="checkbox"/> EYDAP | <input type="checkbox"/> PROS | <input type="checkbox"/> LIF |
| <input type="checkbox"/> CEA | <input type="checkbox"/> VICOM | <input type="checkbox"/> DBC |
| <input type="checkbox"/> DFKI | <input type="checkbox"/> SINTEF | <input type="checkbox"/> CENTRIC |
| <input type="checkbox"/> INTER | <input type="checkbox"/> CERTH | |

Clarifications:

- Exploitation refers to activities planned after the project's completion and represents your aspirations for the future.
- These intentions are not binding obligations but rather a vision of potential opportunities if all necessary resources, funding, and support were available to your organization. Feel free to identify as many goals as you envision, even if only some of them are eventually implemented. For example, if you foresee pursuing 10 objectives but only achieve 5, it is perfectly fine to outline all 10 in your response.
- You can review or update your responses at any time and at your own convenience.
- Some questions require brief answers (2 sentences or up to 100 characters). If a question doesn't apply, simply write 'N/A,' 'none,' or similar to proceed. If you have multiple exploitation plans or ideas, feel free to complete the survey more than once.
- Remember, there are no wrong answers – we are interested in your genuine business insights.

Identification of the target customer of TESTUDO project

Please provide the target customer for your idea/technology, or more broadly, who would be interested in adopting, funding, or purchasing it.

2. Please select your target costumers from the following or write it in the box.

- ☐ End Users
- ☐ EU agencies
- ☐ National governments
- ☐ IT providers
- ☐ Technical innovators
- ☐ Policy makers/ agencies
- ☐ Industry security market operators
- ☐ Manufacturing
- ☐ Academic institutes
- ☐ SMEs
- ☐ Research Institutes
- ☐ Other (please specify):

3. Please provide examples of these customers if required (ie drone operators, security providers etc)

4. When considering a 'broader' customer or adopter, what types do you envision? (You may select multiple options if applicable.)

- ☐ Customer who would potentially pay
- ☐ Customer for free (example: OpenSource)
- ☐ Adopter of our Usecase/ Pilot who would replicate the pilot in their premises
- ☐ Adopter of Research idea
- ☐ Governmental adopter – policy maker or standardisation body
- ☐ Trial adopter
- ☐ Other (please specify):

Initial Market Analysis

Estimate the exploitation idea

5. How would you define the market targeted by your exploitation idea? (This may differ from the market addressed by the overall project.)

- ☐ No market exists yet: The market does not currently exist, and it is uncertain whether our innovations can create one
- ☐ Market-creating: The market does not currently exist, but shows clear potential to be created
- ☐ Emerging: There is a growing demand for solutions like this, with only a few available options
- ☐ Mature: The market is well-established and already offers many alternative products
- ☐ Congested: The market is crowded with numerous offerings from established competitors

6. The market size for your exploitation idea is:

- ☐ Almost none
- ☐ Isolated few
- ☐ Some exist
- ☐ Quite common
- ☐ Many alternatives
- ☐ I don't know

7. Regarding the wider competition, others may have offerings similar to yours. These are primarily:

- ☐ Direct competitors already operating in the market
- ☐ Similar research initiatives, projects, or clusters
- ☐ Potential collaborators with whom we could partner or join forces
- ☐ Alternatives that use different technologies or ideas instead of our solutions
- ☐ Substitutes that don't offer similar solutions but address the same problems in more basic or traditional ways

Please provide a few examples in the box below:



- 8. Please assess the current competition or alternatives to your exploitation idea, including research projects with similar or lower TRL than yours.**

How common are they?

- ☐Almost none
- ☐Isolated few
- ☐Some exist
- ☐Quite common
- ☐Many alternatives
- ☐I don't know

- 9. Please assess the current competition or alternatives to your exploitation idea, including research projects with similar or lower TRL than yours.**

How mature are they?

- ☐Weak (concepts only)
- ☐Somewhat weak (research level/lab trials)
- ☐Average (pilot/use case similar to TESTUDO)
- ☐Strong (many pilots and real world deployments)
- ☐Very strong (various real world deployments)
- ☐I don't know

10. Additional comments you may have